

UNIVERGE WL

V1
(WL1700-MS)

Command Reference

LIABILITY DISCLAIMER

NEC Infrontia Corporation reserves the right to change the specifications, functions, or features, at any time, without notice.

NEC Infrontia Corporation has prepared this document for use by its employees and customers. The information contained herein is the property of NEC Infrontia Corporation, and shall not be reproduced without prior written approval from NEC Infrontia Corporation.

All brand names and product names on this document are trademarks or registered trademarks of their respective companies. For more information about trademarks and service marks, refer to [here](#).

Copyright 2007

NEC Infrontia Corporation



Contents

1	Introducing the UNIVERGE WL System	1
	UNIVERGE WL System	1
	Documentation	2
	Safety and Advisory Notices	3
	Text and Syntax Conventions	3
2	Using the Command-Line Interface	5
	CLI Conventions	6
	Command Prompts	6
	Syntax Notation	7
	Text Entry Conventions and Allowed Characters	7
	MAC Address Notation	8
	IP Address and Mask Notation	8
	Subnet Masks	8
	Wildcard Masks	8
	User Globs, MAC Address Globs, and VLAN Globs	9
	User Globs	9
	MAC Address Globs	10
	VLAN Globs	10
	Matching Order for Globs	11
	Virtual LAN Identification	11
	Command-Line Editing	12
	Keyboard Shortcuts	12
	History Buffer	13
	Tabs	13
	Single-Asterisk (*) Wildcard Character	13
	Double-Asterisk (**) Wildcard Characters	13
	Using CLI Help	14
	Understanding Command Descriptions	15

3	Access Commands	17
4	System Services Commands	21
5	Port Commands	45
6	VLAN Commands	65
7	Quality of Service Commands	89
8	IP Services Commands	95
9	AAA Commands	183
10	Mobility Domain Commands	249
11	Network Domain Commands	257
12	AP Commands	267
13	IGMP Snooping Commands	427
14	Security ACL Commands	453
15	Cryptography Commands	481
16	RADIUS and Server Groups Commands	499
17	802.1X Management Commands	513
18	Session Management Commands	531
19	RF Detection Commands	547
20	File Management Commands	577
21	Trace Commands	605
22	Snoop Commands	613
23	System Log Commands	625
	Index	637

Introducing the UNIVERGE WL System

UNIVERGE WL System	1
Documentation	2

This guide explains how to configure and manage a UNIVERGE WL Wireless Controller (hereinafter called ‘Controller’) using the UNIVERGE WL Control System command line interface (CLI) commands that you enter on a wireless LAN (WLAN) controller.

Read this guide if you are a network administrator or other person configuring and managing one or more UNIVERGE WL Controllers and UNIVERGE WL Access Points in a network.

UNIVERGE WL System

The UNIVERGE WL System an enterprise-class WLAN solution that seamlessly integrates with an existing wired enterprise network. The UNIVERGE WL System provides secure connectivity to both wireless and wired users in large environments such as office buildings, hospitals, and university campuses and in small environments such as branch offices.

The UNIVERGE WL System fulfills the three fundamental requirements of an enterprise WLAN: It eliminates the distinction between wired and wireless networks, allows users to work safely from anywhere (*secure mobility*), and provides a comprehensive suite of intuitive tools for planning and managing the network.

The UNIVERGE WL System consists of the following components:

- 1 **UNIVERGE WLMS**—A full-featured graphical user interface (GUI) application used to plan, configure, deploy, and manage a WLAN and its users
- 1 **UNIVERGE WL Wireless Controller** —Distributed, intelligent machines for managing user connectivity, connecting and powering UNIVERGE WL Access Points, and connecting the WLAN to the wired network backbone
- 1 **UNIVERGE WL Access Points** —Wireless access points (APs) that transmit and receive radio frequency (RF) signals to and from wireless users and connect them to a UNIVERGE WL Wireless Controller
- 1 **UNIVERGE WL Control System** —The operating system that runs all UNIVERGE WL Wireless Controller and UNIVERGE WL Access Points in a WLAN, and is accessible through a command-line interface (CLI), the WebView interface, or the UNIVERGE WLMS GUI

Documentation

Consult the following documents to plan, install, configure, and manage a UNIVERGE WL System.

Planning, Configuration, Deployment and Management

- 1 ***UNIVERGE WLMS User's Guide***. Instructions for planning, configuring, deploying, and managing the entire WLAN with the WLMS tool suite. Read this guide to learn how to plan wireless services, how to configure and deploy UNIVERGE equipment to provide those services, and how to optimize and manage your WLAN.
- 1 ***UNIVERGE WLMS Reference Manual***. Detailed instructions and information for all WLMS planning, configuration, and management features.
- 1 ***UNIVERGE WL Configuration Guide***. Detailed instructions and information for CLI and WebView configuration and management features.
- 1 ***UNIVERGE WL Command Reference*** (this document). Detailed instructions and information for UNIVERGE WL Controller Commands

Installation

- 1 ***UNIVERGE WL Installation Guide***. Instructions and specifications for installing an WL Controller and UNIVERGE WL Access Point

Note. SCA-WL10 has the same specifications as UNIVERGE WL5050.

Safety and Advisory Notices

The following kinds of safety and advisory notices appear in this manual.

Caution! This situation or condition can lead to data loss or damage to the product or other property.

Note. This information is of special interest.

Text and Syntax Conventions

UNIVERGE WL Control System manuals use the following text and syntax conventions:

Convention	Use
Monospace text	Sets off command syntax or sample commands and system responses.
Bold text	Highlights commands that you enter or items you select.
<i>Italic text</i>	Designates command variables that you replace with appropriate values, or highlights publication titles or words requiring special emphasis.
Menu Name > Command	Indicates a menu item that you select. For example, File > New indicates that you select New from the File menu.

Convention

[] (square brackets)

{ } (curly brackets)

| (vertical bar)

Use

Enclose optional parameters in command syntax.

Enclose mandatory parameters in command syntax.

Separates mutually exclusive options in command syntax.

Using the Command-Line Interface

CLI Conventions	6
Command-Line Editing	12
Using CLI Help	14
Understanding Command Descriptions	15

UNIVERGE WL Control System operates a UNIVERGE WL System wireless LAN (WLAN) consisting of WLMS software, UNIVERGE WL Controllers, and UNIVERGE WL Access Points. UNIVERGE WL Control System has a command-line interface (CLI) on the UNIVERGE WL Controller that you can use to configure and manage the UNIVERGE WL Controller and its attached UNIVERGE WL Access Points.

You configure the UNIVERGE WL Controller and the UNIVERGE WL primarily with **set**, **clear**, and **show** commands. Use **set** commands to change parameters. Use **clear** commands to reset parameters to their defaults. In many cases, you can overwrite a parameter with another **set** command. Use **show** commands to display the current configuration and monitor the status of network operations.

The UNIVERGE WL Controller supports two connection modes:

- 1 Administrative access mode, which enables the network administrator to connect *to* the UNIVERGE WL Controller and configure the network
- 1 Network access mode, which enables network users to connect *through* the UNIVERGE WL Controller to access the network

CLI Conventions

Be aware of the following UNIVERGE WL Control System CLI conventions for command entry:

- 1 “Command Prompts” on page 6
- 1 “Syntax Notation” on page 7
- 1 “Text Entry Conventions and Allowed Characters” on page 7
- 1 “User Globs, MAC Address Globs, and VLAN Globs” on page 9
- 1 “Virtual LAN Identification” on page 11

Command Prompts

By default, the UNIVERGE WL Control System CLI provides the following prompt for restricted users. The *mm* portion shows “WL” and the *nnnnnn* portion shows the last 6 digits of the UNIVERGE WL Controller’s media access control (MAC) address.

PROMPT-*mmnnnnnn*>

After you become enabled as an administrative user by typing **enable** and supplying a suitable password, UNIVERGE WL Control System displays the following prompt:

PROMPT-*mmnnnnnn*#

For ease of presentation, this manual shows the restricted and enabled prompts as follows:

PROMPT>

PROMPT#

For information about changing the CLI prompt on a UNIVERGE WL Controller, see **set prompt** on page 31.

Note. When the UNIVERGE WL Controller is in factory default state or after CLI prompt changing, “*” appears at the head of the prompt until the prompt setting is saved.

Syntax Notation

The UNIVERGE WL Control System CLI uses standard syntax notation:

- 1 Bold monospace font identifies the command and keywords you must type. For example:

```
set enablepass
```

- 1 Italic monospace font indicates a placeholder for a value. For example, you replace *vlan-id* in the following command with a virtual LAN (VLAN) ID:

```
clear interface vlan-id ip
```

- 1 Curly brackets ({ }) indicate a mandatory parameter, and square brackets ([]) indicate an optional parameter. For example, you must enter **dynamic** or **port** and a port list in the following command, but a VLAN ID is optional:

```
clear fdb {dynamic | port port-list} [vlan vlan-id]
```

- 1 A vertical bar (|) separates mutually exclusive options within a list of possibilities. For example, you enter either **enable** or **disable**, not both, in the following command:

```
set port {enable | disable} port-list
```

Text Entry Conventions and Allowed Characters

Unless otherwise indicated, the UNIVERGE WL Control System CLI accepts standard ASCII alphanumeric characters, except for tabs and spaces, and is case-insensitive.

The CLI has specific notation requirements for MAC addresses, IP addresses, and masks, and allows you to group usernames, MAC addresses, virtual LAN (VLAN) names, and ports in a single command.

UNIVERGE WL Control System recommends that you do not use the same name with different capitalizations for VLANs or access control lists (ACLs). For example, do not configure two separate VLANs with the names *red* and *RED*.

The CLI does not support the use of special characters including the following in any named elements such as SSIDs and VLANs: ampersand (&), angle brackets (< >), number sign (#), question mark (?), or quotation marks ("").

In addition, the CLI does not support the use of international characters such as the accented *É* in DÉCOR.

MAC Address Notation

UNIVERGE WL Control System displays MAC addresses in hexadecimal numbers with a colon (:) delimiter between bytes—for example, 00:01:02:1a:00:01. You can enter MAC addresses with either hyphen (-) or colon (:) delimiters, but colons are preferred.

For shortcuts:

- 1 You can exclude leading zeros when typing a MAC address. UNIVERGE WL Control System displays of MAC addresses include all leading zeros.
- 1 In some specified commands, you can use the single-asterisk (*) wildcard character to represent from 1 byte to 5 bytes of a MAC address. (For more information, see “MAC Address Globs” on page 10.)

IP Address and Mask Notation

UNIVERGE WL Control System displays IP addresses in dotted decimal notation—for example, 192.168.1.111. UNIVERGE WL Control System makes use of both subnet masks and wildcard masks.

Subnet Masks

Unless otherwise noted, use classless interdomain routing (CIDR) format to express subnet masks—for example, 192.168.1.112/24. You indicate the subnet mask with a forward slash (/) and specify the number of bits in the mask.

Wildcard Masks

Security access control lists (ACLs) use source and destination IP addresses and wildcard masks to determine whether the UNIVERGE WL Controller filters or forwards IP packets. Matching packets are either permitted or denied network access. The ACL checks the bits in IP addresses that correspond to any 0s (zeros) in the mask, but does not check the bits that correspond to 1s (ones) in the mask. You specify the wildcard mask in dotted decimal notation.

For example, the address 10.0.0.0 and mask 0.255.255.255 match all IP addresses that begin with 10 in the first octet.

The ACL mask must be a contiguous set of zeroes starting from the first bit. For example, 0.255.255.255, 0.0.255.255, and 0.0.0.255 are valid ACL masks. However, 0.255.0.255 is not a valid ACL mask.

User Globs, MAC Address Globs, and VLAN Globs

Name “globbing” is a way of using a wildcard pattern to expand a single element into a list of elements that match the pattern. UNIVERGE WL Control System accepts user globs, MAC address globs, and VLAN globs. The order in which globs appear in the configuration is important, because once a glob is matched, processing stops on the list of globs.

User Globs

A user glob is shorthand method for matching an authentication, authorization, and accounting (AAA) command to either a single user or a set of users.

A user glob can be up to 80 characters long and cannot contain spaces or tabs. The double-asterisk (**) wildcard characters with no delimiter characters match *all* usernames. The single-asterisk (*) wildcard character matches any number of characters up to, but not including, a delimiter character in the glob. Valid user glob delimiter characters are the *at* (@) sign and the period (.).

For example, the following globs identify the following users:

User Glob	User(s) Designated
jose@example.com	User <i>jose</i> at example.com
*@example.com	All users at example.com whose usernames do not contain periods—for example, jose@example.com and tamara@example.com, but <i>not</i> nin.wong@example.com, because nin.wong contains a period
*@marketing.example.com	All marketing users at example.com whose usernames do not contain periods

User Glob	User(s) Designated
.@marketing.example.com	All marketing users at example.com whose usernames contain periods
*	All users with usernames that have no delimiters
EXAMPLE*	All users in the Windows Domain EXAMPLE with usernames that have no delimiters
EXAMPLE*.*	All users in the Windows Domain EXAMPLE whose usernames contain periods
**	All users

MAC Address Globs

A media access control (MAC) address glob is a similar method for matching some authentication, authorization, and accounting (AAA) and forwarding database (FDB) commands to one or more 6-byte MAC addresses. In a MAC address glob, you can use a single asterisk (*) as a wildcard to match *all* MAC addresses, or as follows to match from 1 byte to 5 bytes of the MAC address:

```
00:*
00:01:*
00:01:02:*
00:01:02:03:*
00:01:02:03:04:*
```

For example, the MAC address glob 02:06:8c* represents all MAC addresses starting with 02:06:8c. Specifying only the first 3 bytes of a MAC address allows you to apply commands to MAC addresses based on an organizationally unique identity (OUI).

VLAN Globs

A VLAN glob is a method for matching one of a set of local rules on a UNIVERGE WL Controller, known as the location policy, to one or more users. UNIVERGE WL Control System compares the VLAN glob, which can optionally contain wildcard characters, against the VLAN-Name attribute returned by AAA, to determine whether to apply the rule.

To match all VLANs, use the double-asterisk (**) wildcard characters with no delimiters. To match any number of characters up to, but not including, a delimiter character in the glob, use the single-asterisk (*) wildcard. Valid VLAN glob delimiter characters are the *at* (@) sign and the period (.).

For example, the VLAN glob *bldg4.** matches *bldg4.security* and *bldg4.hr* and all other VLAN names with *bldg4.* at the beginning.

Matching Order for Globs

In general, the order in which you enter AAA commands determines the order in which UNIVERGE WL Control System matches the user, MAC address, or VLAN to a glob. To verify the order, view the output of the **show aaa** or **show config** command. UNIVERGE WL Control System checks globs that appear higher in the list before items lower in the list and uses the first successful match.

Virtual LAN Identification

The *names* of virtual LANs (VLANs), which are used in Mobility Domain™ communications, are set by you and can be changed. In contrast, VLAN ID *numbers*, which the UNIVERGE WL Controller uses locally, are determined when the VLAN is first configured and cannot be changed. Unless otherwise indicated, you can refer to a VLAN by either its VLAN name or its VLAN number. CLI **set** and **show** commands use a VLAN's name or number to uniquely identify the VLAN within the UNIVERGE WL Controller.

Command-Line Editing

UNIVERGE WL Control System editing functions are similar to those of many other network operating systems.

Keyboard Shortcuts

The following table lists the keyboard shortcuts for entering and editing CLI commands:

Keyboard Shortcut(s)	Function
Ctrl+A	Jumps to the first character of the command line.
Ctrl+B or Left Arrow key	Moves the cursor back one character.
Ctrl+C	Escapes and terminates prompts and tasks.
Ctrl+D	Deletes the character at the cursor.
Ctrl+E	Jumps to the end of the current command line.
Ctrl+F or Right Arrow key	Moves the cursor forward one character.
Ctrl+K	Deletes from the cursor to the end of the command line.
Ctrl+L or Ctrl+R	Repeats the current command line on a new line.
Ctrl+N or Down Arrow key	Enters the next command line in the history buffer.
Ctrl+P or Up Arrow key	Enters the previous command line in the history buffer.
Ctrl+U or Ctrl+X	Deletes characters from the cursor to the beginning of the command line.
Ctrl+W	Deletes the last word typed.
Esc B	Moves the cursor back one word.
Esc D	Deletes characters from the cursor forward to the end of the word.
Delete key or Backspace key	Erases mistake made during command entry. Reenter the command after using this key.

History Buffer

The history buffer stores the last 63 commands you entered during a terminal session. You can use the Up Arrow and Down Arrow keys to select a command that you want to repeat from the history buffer.

Tabs

The UNIVERGE WL Control System CLI uses the Tab key for command completion. You can type the first few characters of a command and press the Tab key to display the command(s) that begin with those characters. For example:

```
PROMPT# show i <Tab>
igmp      Show igmp information
interface Show interfaces
ip        Show ip information
```

Single-Asterisk (*) Wildcard Character

You can use the single-asterisk (*) wildcard character in globbing. (For details, see “User Globs, MAC Address Globs, and VLAN Globs” on page 9.)

Double-Asterisk (**) Wildcard Characters

The double-asterisk (**) wildcard character matches all usernames. For details, see “User Globs” on page 9.

Using CLI Help

The CLI provides online help. To see the full range of commands available at your access level, type the **help** command. For example:

PROMPT# **help**

Commands:

```
-----
clear          Clear, use 'clear help' for more information
commit         Commit the content of the ACL table
copy           Copy from filename (or url) to filename (or url)
crypto         Crypto, use 'crypto help' for more information
delete         Delete url
dir            Show list of files on flash device
disable        Disable privileged mode
exit           Exit from the Admin session
help           Show this help screen
history        Show contents of history substitution buffer
load           Load, use 'load help' for more information
logout         Exit from the Admin session
monitor        Monitor, use 'monitor help' for more information
ping           Send echo packets to hosts
quit           Exit from the Admin session
reset          Reset, use 'reset help' for more information
rollback       Remove changes to the edited ACL table
save           Save the running configuration to persistent storage
set            Set, use 'set help' for more information
show           Show, use 'show help' for more information
telnet         telnet IP address [server port]
traceroute     Print the route packets take to network host
```

For more information on help, see **help** on page 25.

To see a subset of the online help, type the command for which you want more information. For example, to display all the commands that begin with the letter *i*, type the following command:

PROMPT# **show i?**

```
igmp          Show igmp information
interface     Show interfaces
ip            Show ip information
```

To see all the variations, type one of the commands followed by a question mark (?). For example:

PROMPT# **show ip ?**

```
alias         Show ip aliases
```

dns	show DNS status
https	show ip https
route	Show ip route table
telnet	show ip telnet

To determine the port on which Telnet is running, type the following command:

```
PROMPT# show ip telnet
Server Status      Port
-----
Enabled            23
```

Understanding Command Descriptions

Each command description in the *WL Command Reference* contains the following elements:

- 1 A command name, which shows the keywords but not the variables. For example, the following command name appears at the top of a command description and in the index:

`set ap name`
- 1 A brief description of how the command functions.
- 1 The full command syntax.
- 1 Any command defaults.
- 1 The command access, which is either *enabled* or *all*. *All* indicates that anyone can access this command. *Enabled* indicates that you must enter the enable password before entering the command.
- 1 The command history, which identifies the UNIVERGE WL Control System version in which the command was introduced and the version numbers of any subsequent updates.
- 1 Special tips for command usage. These are omitted if the command requires no special usage.
- 1 One or more examples of the command in context, with the appropriate system prompt and response.
- 1 One or more related commands.

Access Commands

Use access commands to control access to the UNIVERGE WL Control System (CLI). This chapter presents access commands alphabetically. Use the following table to locate commands in this chapter based on their use.

Access Privileges	enable on page 17
	set enablepass on page 19
	disable on page 17
	quit on page 18

disable

Changes the CLI session from enabled mode to restricted access.

Syntax `disable`

Defaults None.

Access Enabled.

Examples The following command restricts access to the CLI for the current session:

```
PROMPT# disable
PROMPT>
```

See Also `enable` on page 17

enable

Places the CLI session in enabled mode, which provides access to all commands required for configuring and monitoring the system.

quit

Chapter 3

Syntax `enable`

Access All.

Usage UNIVERGE WL Control System displays a password prompt to challenge you with the enable password. To enable a session, your or another administrator must have configured the enable password to this UNIVERGE WL Controller with the `set enablepass` command.

Examples The following command plus the enable password provides enabled access to the CLI for the current sessions:

```
PROMPT> enable
Enter password: password
PROMPT#
```

See Also

1 `set enablepass` on page 19

1 `set confirm` on page 29

quit

Exit from the CLI session.

Syntax `quit`

Defaults None.

Access All.

Examples To end the administrator's session, type the following command:

```
PROMPT> quit
```

set enablepass

Sets the password that provides enabled access (for configuration and monitoring) to the UNIVERGE WL Controller.



Note. The enable password is case-sensitive.

Syntax set enablepass

Defaults None.

Access Enabled.

Usage After typing the **set enablepass** command, press Enter. If you are entering the first enable password on this UNIVERGE WL Controller, press Enter at the *Enter old password* prompt. Otherwise, type the old password. Then type a password of up to 32 alphanumeric characters with no spaces, and reenter it at the *Retype new password* prompt.



Caution! Be sure to use a password that you will remember. If you lose the enable password, the only way to restore it causes the system to return to its default settings and wipes out the configuration.

Examples The following example illustrates the prompts that the system displays when the enable password is changed. The passwords you enter are not displayed.

PROMPT# set enablepass

```
Enter old password: old-password
Enter new password: new-password
Retype new password: new-password
success: Password changed
```

See Also

1 **disable** on page 17

1 **enable** on page 17

set enablepass

Chapter 3

System Services Commands

Use system services commands to configure and monitor system information for a UNIVERGE WL Controller. This chapter presents system services commands alphabetically. Use the following table to located commands in this chapter based on their use.

Auto-Config	set auto-config on page 26
Display	clear banner motd on page 22
	set banner motd on page 29
	show banner motd on page 39
	set confirm on page 29
	set length on page 30
System Identification	set prompt on page 31
	set system name on page 38
	set system location on page 37
	set system contact on page 32
	set system countrycode on page 33
	set system idle-timeout on page 35
	set system ip-address on page 36
	show load on page 39
	show system on page 40
	clear system on page 23
	clear prompt on page 23
Help	help on page 25
History	history on page 26

	clear history on page 22
License	set license on page 31
	show license on page 39
Technical Support	show tech-support on page 44

clear banner motd

Deletes the message-of-the-day (MOTD) banner that is displayed before the login prompt for each CLI session on the UNIVERGE WL Controller.

Syntax **clear banner motd**

Defaults None.

Access Enabled.

Examples To clear a banner, type the following command:

```
PROMPT# clear banner motd
success: change accepted
```



Note. As an alternative to clearing the banner, you can overwrite the existing banner with an empty banner by typing the following command: **set banner motd ^^**

See Also

- 1 **set banner motd** on page 29
- 1 **show banner motd** on page 39

clear history

Deletes the command history buffer for the current CLI session.

Syntax **clear history**

Defaults None.

Access All.

Examples To clear the history buffer, type the following command:

```
PROMPT# clear history
success: command buffer was flushed.
```

See Also **history** on page 26

clear prompt

Resets the system prompt to its previously configured value. If the prompt was not configured previously, this command resets the prompt to its default.

Syntax **clear prompt**

Defaults None.

Access Enabled.

Examples To reset the prompt, type the following command:

```
wildebeest# clear prompt
success: change accepted.
PROMPT#
```

See Also **set prompt** on page 31. (For information about default prompts, see “Command Prompts” on page 6.)

clear system

Clears the system configuration of the specified information.



Caution! If you change the IP address, any currently configured Mobility Domain operations cease. You must reset the Mobility Domain.

Syntax **clear system** [**contact** | **countrycode** | **idle-timeout** | **ip-address** | **location** | **name**]

contact	Resets the name of contact person for the UNIVERGE WL Controller to null.
countrycode	Resets the country code for the UNIVERGE WL Controller to null.
idle-timeout	Resets the number of seconds a CLI management session can remain idle to the default value (3600 seconds).
ip-address	Resets the IP address of the UNIVERGE WL Controller to null.
location	Resets the location of the UNIVERGE WL Controller to null.
name	Resets the name of the UNIVERGE WL Controller to the default system name, which is <i>UNIVERGE-mm-nnnnnnn</i> , where <i>mm</i> is the model number and <i>nnnnnnn</i> is the last 6 digits of the UNIVERGE WL Controller's MAC address.

Defaults None.

Access Enabled.

Examples To clear the location of the UNIVERGE WL Controller, type the following command:

```
PROMPT# clear system location
success: change accepted.
```

See Also

- 1 **set system contact** on page 32
- 1 **set system countrycode** on page 33
- 1 **set system idle-timeout** on page 35
- 1 **set system ip-address** on page 36
- 1 **set system location** on page 37
- 1 **show config** on page 600

1 **show system** on page 40

help

Displays a list of commands that can be used to configure and monitor the UNIVERGE WL Controller.

Syntax **help**

Defaults None.

Access All.

Examples Use this command to see a list of available commands. If you have restricted access, you see fewer commands than if you have enabled access. To display a list of CLI commands available at the enabled access level, type the following command at the enabled access level:

PROMPT# help
Commands:

```
-----
clear          Clear, use 'clear help' for more information
commit        Commit the content of the ACL table
copy          Copy from filename (or url) to filename (or url)
crypto        Crypto, use 'crypto help' for more information
delete        Delete url
dir           Show list of files on flash device
disable       Disable privileged mode
exit          Exit from the Admin session
help          Show this help screen
history       Show contents of history substitution buffer
load          Load, use 'load help' for more information
logout        Exit from the Admin session
monitor       Monitor, use 'monitor help' for more information
ping          Send echo packets to hosts
quit          Exit from the Admin session
reset         Reset, use 'reset help' for more information
rollback      Remove changes to the edited ACL table
save          Save the running configuration to persistent storage
set           Set, use 'set help' for more information
show          Show, use 'show help' for more information
telnet        telnet IP address [server port]
traceroute    Print the route packets take to network host
```

See Also “Using CLI Help” on page 14

history

Displays the command history buffer for the current CLI session.

Syntax **history**

Defaults None.

Access All.

Examples To show the history of your session, type the following command:

```
PROMPT> history
Show History (most recent first)
-----
[00] show config
[01] show version
[02] enable
```

See Also **clear history** on page 22

set auto-config

Enables a UNIVERGE WL Controller to contact a WLMS server for its configuration.

Syntax **set auto-config {enable | disable}**

enable Enables the UNIVERGE WL Controller to contact a WLMS server to request a configuration.

disable Disables the auto-config option.

Defaults The auto-config option is disabled by default.

Access Enabled.

Usage A network administrator at the corporate office can preconfigure the UNIVERGE WL Controller in a WLMS network plan. The UNIVERGE WL Controller configuration must have a name for the UNIVERGE WL Controller, the serial number must match the UNIVERGE WL Controller's serial number. The configuration should also include all other settings required for the deployment, including UNIVERGE WL Access Points configuration, SSIDs, AAA settings, and so on.

When the WLMS server in the corporate network receives the configuration request, the server looks in the currently open network plan for a UNIVERGE WL Controller configuration with the same model and serial number as the one in the configuration request.

- 1 If the network plan contains a configuration with a matching model and serial number, WLMS sends the configuration to the UNIVERGE WL Controller and restarts the UNIVERGE WL Controller. The UNIVERGE WL Controller boots using the configuration it received from WLMS.
- 1 If the network plan does not have a configuration with a matching model and serial number, a verification warning appears in WLMS. The warning lists the UNIVERGE WL Controller's serial number and IP address. The network administrator can upload the UNIVERGE WL Controller into the network plan, configure UNIVERGE WL Controller parameters, and deploy the configuration to the UNIVERGE WL Controller.

UNIVERGE WL Controller model to be able to access a WLMS server for a configuration, you also must preconfigure the UNIVERGE WL Controller with the following information:

- 1 IP address
- 1 Default router (gateway) address
- 1 Domain name and DNS server address

You can enable the UNIVERGE WL Controller to use the UNIVERGE WL Control System DHCP client to obtain this information from a DHCP server in the local network where the UNIVERGE WL Controller will be deployed. Alternatively, you can statically configure the information.

The IP address and DNS information are configured independently. You can configure the combination of settings that work with the network resources available at the deployment site. The following examples show some of the combinations you can configure.

Examples The following commands stage a UNIVERGE WL Controller to use the auto-config option. The network where the UNIVERGE WL Controller is installed has a DHCP server, so the UNIVERGE WL Controller is configured to use the UNIVERGE WL Control System DHCP client to obtain an IP address, default router address, DNS domain name, and DNS server IP addresses.

1 Configure a VLAN:

```
PROMPT# set vlan 1 port 1
success: change accepted.
```

2 Enable the DHCP client on VLAN 1:

```
PROMPT# set interface 1 ip dhcp-client enable
success: change accepted.
```

3 Enable the auto-config option:

```
PROMPT# set auto-config enable
success: change accepted.
```

4 Save the configuration changes:

```
PROMPT# save config
success: configuration saved.
```

See Also

- 1 **crypto generate key** on page 485
- 1 **crypto generate self-signed** on page 489
- 1 **save config** on page 594
- 1 **set interface dhcp-client** on page 112
- 1 **set vlan port** on page 75

set banner motd

Configures the banner string that is displayed before the beginning of each login prompt for each CLI session on the UNIVERGE WL Controller.

Syntax `set banner motd "text"`

“ Delimiting character that begins and ends the message; for example, double quotes (“”).

text Up to 4096 alphanumeric characters, including tabs and carriage returns, but not the delimiting character.

Defaults None.

Access Enabled.

Usage Type a delimiting character, then the message, then another delimiting character.

Examples To create a banner that says *Meeting @ 4:00 p.m.* in Conference Room #3, type the following command:

```
PROMPT# set banner motd "Meeting @ 4:00 p.m. in Conference Room #3"
success: motd changed.
```

See Also

1 **clear banner motd** on page 22

1 **show banner motd** on page 39

set confirm

Enables or disables the display of confirmation messages for commands that might have a large impact on the network.

Syntax `set confirm {on | off}`

on Enables confirmation messages.

off Disables confirmation messages.

set length

Chapter 4

Defaults Configuration messages are enabled.

Access Enabled.

Usage This command remains in effect for the duration of the session, until you enter an **exit** or **quit** command, or until you enter another **set confirm** command.

UNIVERGE WL Control System displays a message requiring confirmation when you enter certain commands that can have a potentially large impact on the network. For example:

```
PROMPT# clear vlan red
This may disrupt user connectivity. Do you wish to continue? (y/n) [n]
```

Examples To turn off these confirmation messages, type the following command:

```
PROMPT# set confirm off
success: Confirm state is off
```

set length

Defines the number of lines of CLI output to display between paging prompts. UNIVERGE WL Control System displays the set number of lines and waits for you to press any key to display another set, or type **q** to quit the display.

Syntax **set length** *number-of-lines*

number-of-lines Number of lines of text to display between paging prompts. You can specify from 0 to 512. The 0 value disables the paging prompt action entirely.

Defaults UNIVERGE WL Control System displays 24 lines by default.

Access All.

Usage Use this command if the output of a CLI command is greater than the number of lines allowed by default for a terminal type.

Examples To set the number of lines displayed to 100, type the following command:

```
PROMPT# set length 100
success: screen length for this session set to 100
```

set license

Installs an upgrade license key on a UNIVERGE WL Controller.



Note. This command is not supported.

set prompt

Changes the CLI prompt for the UNIVERGE WL Controller to a string you specify.

Syntax `set prompt string`

string Alphanumeric string up to 32 characters long. To include spaces in the prompt, you must enclose the string in double quotation marks (“”).

Defaults The factory default for the UNIVERGE WL Controller name is UNIVERGE-*nnnnnnn*, where *mm* is the model number and *nnnnnnn* is the last 6 digits of the 12-digit system MAC address.

Access Enabled.

Usage When you first log in for the initial configuration of the UNIVERGE WL Controller, the CLI provides a UNIVERGE_*nnnnnnn*> prompt. After you become enabled by typing **enable** and giving a suitable password, the UNIVERGE-*nnnnnnn*# prompt is displayed.

If you use the **set system name** command to change the default system name, UNIVERGE WL Control System uses that name in the prompt, unless you also change the prompt with **set prompt**.

Examples The following example sets the prompt from UNIVERGE WL Controller to *happy_days*:

```
UNIVERGE_nnnnnn# set prompt happy_days
success: change accepted.
happy_days#
```

set system contact

Chapter 4

See Also

- 1 **clear prompt** on page 23
- 1 **set system name** on page 38
- 1 **show config** on page 600

set system contact

Stores a contact name for the UNIVERGE WL Controller.

Syntax **set system contact** *string*

string Alphanumeric string up to 256 characters long. (blank spaces are available to input.)

Defaults None.

Access Enabled.

To view the system contact string, type the **show system** command.

Examples The following command sets the system contact information to *tamara@example.com*:

```
Controller#set system contact tamara@example.com
success: change accepted.
```

See Also

- 1 **clear system** on page 23
- 1 **set system location** on page 37
- 1 **set system name** on page 38
- 1 **show system** on page 40

set system countrycode

Defines the country-specific IEEE 802.11 regulations to enforce on the UNIVERGE WL Controller.

Syntax `set system countrycode code`

code Two-letter code for the country of operation for the UNIVERGE WL Controller. You can specify one of the codes listed in Table 1.

Table 1. Country Codes

Country	Code
Australia	AU
Austria	AT
Belgium	BE
Brazil	BR
Canada	CA
China	CN
Czech Republic	CZ
Denmark	DK
Finland	FI
France	FR
Germany	DE
Greece	GR
Hong Kong	HK
Hungary	HU
Iceland	IS
India	IN
Ireland	IE

Table 1. Country Codes

Country	Code
Israel	IL
Italy	IT
Japan	JP
Liechtenstein	LI
Luxembourg	LU
Malaysia	MY
Mexico	MX
Netherlands	NL
New Zealand	NZ
Norway	NO
Poland	PL
Portugal	PT
Saudi Arabia	SA
Singapore	SG
Slovakia	SK
Slovenia	SI
South Africa	ZA
South Korea	KR
Spain	ES
Sweden	SE
Switzerland	CH
Taiwan	TW
Thailand	TH
United Arab Emirates	AE
United Kingdom	GB
United States	US

Defaults The factory default country code is *None*.

Access Enabled.

Usage You must set the system country code to a valid value before using any **set ap** commands to configure a UNIVERGE WL Access Points.

Examples To set the country code to Canada, type the following command:

```
Controller#set system country code CA
success: change accepted.
```



Note. Under no circumstances should you specify a country code that does not match the country of operation. If the country of operation is not listed in Table 1, this might be because the country has not yet approved the use of this equipment. In this case, contact your local supplier before installing the equipment.

See Also **show config** on page 600

set system idle-timeout

Specifies the maximum number of seconds a CLI management session with the UNIVERGE WL Controller can remain idle before UNIVERGE WL Control System terminates the session.

Syntax **set system idle-timeout** *seconds*

seconds Number of seconds a CLI management session can remain idle before UNIVERGE WL Control System terminates the session. You can specify from 0 to 86400 seconds (one day). If you specify 0, the idle timeout is disabled.

The timeout interval is in 30-second increments. For example, the interval can be 0, or 30 seconds, or 60 seconds, or 90 seconds, and so on. If you enter an interval that is not divisible by 30, the CLI rounds up to the next 30-second increment. For example, if you enter 31, the CLI rounds up to 60.

Defaults 3600 seconds (one hour).

set system ip-address

Chapter 4

Access Enabled.

Usage This command applies to all types of CLI management sessions: console, Telnet, and SSH. The timeout change applies to existing sessions only, not to new sessions.

Examples The following command sets the idle timeout to 1800 seconds (one half hour):

```
PROMPT# set system idle-timeout 1800
success: change accepted.
```

See Also

1 **clear system** on page 23

1 **show system** on page 40

set system ip-address

Sets the system IP address so that it can be used by various services in the UNIVERGE WL Controller.



Caution! Any currently configured Mobility Domain operations cease if you change the IP address. If you change the address, you must reset the Mobility Domain.

Syntax **set system ip-address** *ip-addr*

ip-addr IP address, in dotted decimal notation.

Defaults None.

Access Enabled.

Examples The following command sets the IP address of the UNIVERGE WL Controller to 192.168.253.1:

```
PROMPT# set system ip-address 192.168.253.1
This will cause all APs to reboot. Are you sure? (y/n) [n]y
success: change accepted.
```

See Also

- 1 **clear system** on page 23
- 1 **set interface** on page 111
- 1 **show system** on page 40

set system location

Stores location information for the UNIVERGE WL Controller.

Syntax **set system location** *string*

string Alphanumeric string up to 256 characters long. (blank spaces are available to input.)

Defaults None.

Access Enabled.

Usage You cannot include spaces in the system location string. To view the system location string, type the **show system** command.

Examples To store the location of the UNIVERGE WL Controller in the UNIVERGE WL Controller's configuration, type the following command:

```
PROMPT# set system location first-floor-bldg3
success: change accepted.
```

See Also

- 1 **clear system** on page 23
- 1 **set system contact** on page 32
- 1 **set system name** on page 38
- 1 **show system** on page 40

set system name

Changes the name of the UNIVERGE WL Controller from the default system name and also provides content for the CLI prompt, if you do not specify a prompt.

Syntax **set system name** *string*

string Alphanumeric string up to 99 characters long. (blank spaces are available to input.) UNIVERGE WLMS requires unique UNIVERGE WL Controller names.

Defaults By default, the system name and command prompt have the same value. The factory default for both is *UNIVERGE-mm_nnnnnnn*, where *mm* is the model number and *nnnnnnn* is the last 6 digits of the 12-digit system MAC address.

Access Enabled.

Usage Entering **set system name** with no string resets the system name to the factory default.

To view the system name string, type the **show system** command.

Examples The following example sets the system name to a name that identifies the UNIVERGE WL Controller:

```
PROMPT# set system name WL-bldg3
success: change accepted.
WL-bldg3#
```

See Also

- 1 **clear system** on page 23
- 1 **set prompt** on page 31
- 1 **set system contact** on page 32
- 1 **set system location** on page 37
- 1 **show system** on page 40

show banner motd

Shows the banner that was configured with the **set banner motd** command.

Syntax **show banner motd**

Defaults None.

Access Enabled.

Examples To display the banner with the message of the day, type the following command:

```
PROMPT# show banner motd  
hello world
```

See Also

1 **clear banner motd** on page 22

show license



Note. This command is not supported.

show load

Displays CPU usage on a UNIVERGE WL Controller.

Syntax **show load**

Defaults None.

Access Enabled.

Examples To display the CPU load recorded from the time the UNIVERGE WL Controller was booted, as well as from the previous time the **show load** command was run, type the following command:

```
PROMPT# show load  
System Load: overall: 2% delta: 5%
```

show system

Chapter 4

The overall field shows the CPU load as a percentage from the time the UNIVERGE WL Controller was booted. The delta field shows CPU load as a percentage from the last time the **show load** command was entered.

See Also **show system** on page 40

show system

Displays system information.

Syntax **show system**

Defaults None.

Access Enabled.

Examples To show system information, type the following command:

```
PROMPT# show system
=====
Product Name:          WL5100
System Name:           WL-bldg3
System Country Code:   US
System Location:       first-floor-bldg3
System Contact:        tamara@example.com
System IP Address:     192.168.12.7
System Idle Timeout [s]: 1800
System MAC:            00:30:13:63:DD:3C
Hardware Key:          133303330164D01D220058D41CAK
=====
Boot Time:             2006-09-16 03:06:04
Uptime:                4 days 15:51:55
=====
Fan Status:            Fan OK.
Temperature:           Temp1 OK Temp2 OK.
PSU Status:            Left Power Supply AC OK DC OK Right Power Supply AC OK DC OK.
Memory [MB]:           351.09/1003.01 (35%)
=====
```

Table 2 describes the fields of **show system** output.

Table 2. show system Output

Field	Description
Product Name	UNIVERGE WL Controller model number.
System Name	System name (factory default, or optionally configured with set system name).
System Countrycode	Country-specific 802.11 code required for AP operation (configured with set system countrycode).
System Location	Record of UNIVERGE WL Controller's physical location (optionally configured with set system location).
System Contact	Contact information about the system administrator or another person to contact about the system (optionally configured with set system contact).
System IP Address	Common interface, source, and default IP address for the UNIVERGE WL Controller, in dotted decimal notation (configured with set system ip-address).
System idle timeout	Number of seconds UNIVERGE WL Control System allows a CLI management session (console, Telnet, or SSH) to remain idle before terminating the session. (The system idle timeout can be configured using the set system idle-timeout command.)
System MAC	UNIVERGE WL Controller media access control (MAC) machine address set at the factory, in 6-byte hexadecimal format.
Hardware Key	UNIVERGE WL Controller Hardware Key in the WL5100. It is an unique number every UNIVERGE WL Controller.
Boot Time	Date and time of the last system reboot.
Uptime	Number of days, hours, minutes, and seconds that the UNIVERGE WL Controller has been operating since its last restart.

Table 2. show system Output

Field	Description
Fan status	<p>Operating status of the three WL5100 cooling fans:</p> <ul style="list-style-type: none"> • OK—Fan is operating. • Failed—Even as for 1 in three fan in the case of not operating. UNIVERGE WL Control System sends an alert to the system log every 5 minutes until this condition is corrected. <p>Fan 1 is located nearest the front of the chassis, and fan 3 is located nearest the back.</p> <p>In the case of WL1700-MS, nothing is displayed.</p>
Temperature	<p>Status of temperature sensors at three locations in the WL5100:</p> <p>temp1</p> <ul style="list-style-type: none"> • ok—Temperature is within the acceptable range of 5° C to 100° C (32° F to 212° F). • ng—Temperature is above or below the acceptable range. <p>temp2</p> <ul style="list-style-type: none"> • ok—Temperature is within the acceptable range of 0° C to 60° C (41° F to 140° F). • ng—Temperature is above or below the acceptable range. • Alarm—Temperature is above or below the acceptable range. UNIVERGE WL Control System sends an alert to the system log every 5 minutes until this condition is corrected.
SCA-WL10 WL1700-MS	<p>Status of the one power supply units in the SCA-WL10 and WL1700-MS:</p> <ul style="list-style-type: none"> • DC ok—Power supply is producing DC power.
PSU Status	<ul style="list-style-type: none"> • DC output failure—Power supply is not producing DC power. UNIVERGE WL Control System sends an alert to the system log every 5 minutes until this condition is corrected. • AC ok—Power supply is receiving AC power. • AC not present—Power supply is not receiving AC power.

Table 2. show system Output

Field	Description
WL5100	Status of the Left and Right power supply units in the WL5100:
PSU Status	<ul style="list-style-type: none"> • missing—Power supply is not installed or is inoperable. • DC ok—Power supply is producing DC power. • DC output failure—Power supply is not producing DC power. UNIVERGE WL Control System sends an alert to the system log every 5 minutes until this condition is corrected. • AC ok—Power supply is receiving AC power. • AC not present—Power supply is not receiving AC power.
Memory	<p>Current size (in megabytes) of nonvolatile memory (NVRAM) and synchronous dynamic RAM (SDRAM), plus the percentage of total memory space in use, in the following format:</p> <p><i>NVRAM size /SDRAM size (percent of total)</i></p>

See Also

- 1 **clear system** on page 23
- 1 **set system contact** on page 32
- 1 **set system countrycode** on page 33
- 1 **set system idle-timeout** on page 35
- 1 **set system ip-address** on page 36
- 1 **set system location** on page 37
- 1 **set system name** on page 38

show tech-support

Provides an in-depth snapshot of the status of the UNIVERGE WL Controller, which includes details about the boot image, the version, ports, and other configuration values. This command also displays the last 100 log messages.

Syntax **show tech-support** [**file** *[subdirname/]filename*]

<i>[subdirname/]filename</i>	Optional subdirectory name, and a string up to 32 alphanumeric characters. The command's output is saved into a file with the specified name in nonvolatile storage.
------------------------------	--

Defaults None.

Access Enabled.

Usage Enter this command before calling the UNIVERGE Technical Assistance Center (TAC).

See Also

- 1 **show boot** on page 597
- 1 **show config** on page 600
- 1 **show license** on page 39
- 1 **show system** on page 40
- 1 **show version** on page 602

Port Commands

This chapter presents port commands alphabetically. Use the following table to locate commands in this chapter based on their use.

Port Type	clear ap on page 45
Name	set port name on page 57
	clear port name on page 47
State	set port on page 55
	reset port on page 53
	show port status on page 63
Speed	set port speed on page 60
Autonegotiation	set port negotiation on page 58
SNMP	set port trap on page 61
Statistics	show port counters on page 62
	monitor port counters on page 47
	clear port counters on page 46

clear ap



Caution! When you clear a UNIVERGE WL Access Points, UNIVERGE WL Control System ends user sessions that are using the UNIVERGE WL Access Points.

Removes a UNIVERGE WL Access Points.

clear port counters

Chapter 5

Syntax **clear ap** {*ap-number* / **all**}

ap-number Number of the UNIVERGE WL Access Points to be removed.

all Clear all UNIVERGE WL Access Points.

Defaults None.

Access Enabled.

Examples The following command clears UNIVERGE WL Access Points 1:

```
PROMPT# clear ap 1
This will clear specified AP devices. Would you like to continue? (y/n) [n]y
```

See Also

1 **set ap** on page 54

clear port counters

Clears port statistics counters and resets them to 0.

Syntax **clear port counters**

Defaults None.

Access Enabled.

Examples The following command clears all port statistics counters and resets them to 0:

```
PROMPT# clear port counters
success: cleared port counters
```

See Also

1 **monitor port counters** on page 47

1 **show port counters** on page 62

clear port name

Removes the name assigned to a port.

Syntax `clear port port-list name`

port-list List of physical ports. UNIVERGE WL Control System removes the names from all the specified ports.

Defaults None.

Access Enabled.

Examples The following command clears the names of ports 1:

```
PROMPT# clear port 1 name
```

See Also

1 **set port name** on page 57

1 **show port status** on page 63

monitor port counters

Displays and continually updates port statistics.

Syntax `monitor port counters [octets | packets | receive-errors | transmit-errors | collisions | receive-etherstats | transmit-etherstats]`

octets Displays octet statistics first.

packets Displays packet statistics first.

receive-errors Displays errors in received packets first.

transmit-errors Displays errors in transmitted packets first.

collisions Displays collision statistics first.

monitor port counters

Chapter 5

receive-etherstats	Displays Ethernet statistics for received packets first.
transmit-etherstats	Displays Ethernet statistics for transmitted packets first.

Defaults All types of statistics are displayed for ports. UNIVERGE WL Control System refreshes the statistics every 5 seconds, and the interval cannot be configured. Statistics types are displayed in the following order by default:

- 1 Octets
- 1 Packets
- 1 Receive errors
- 1 Transmit errors
- 1 Collisions
- 1 Receive Ethernet statistics
- 1 Transmit Ethernet statistics

Access All.

Usage Each type of statistic is displayed separately. Press the Spacebar to cycle through the displays for each type.

If you use an option to specify a statistic type, the display begins with that statistic type. You can use one statistic option with the command.

Use the keys listed in Table 3 to control the monitor display.

Table 3. Key Controls for Monitor Port Counters Display

Key	Effect on Monitor Display
Spacebar	Advances to the next statistic type.

Table 3. Key Controls for Monitor Port Counters Display

Key	Effect on Monitor Display
Esc	Exits the monitor. UNIVERGE WL Control System stops displaying the statistics and displays a new command prompt.
c	Clears the statistics counters for the currently displayed statistics type. The counters begin incrementing again.

For error reporting, the cyclic redundancy check (CRC) errors include misalignment errors. Jumbo packets with valid CRCs are not counted. A short packet can be reported as a short packet, a CRC error, or an overrun. In some circumstances, the transmitted octets counter might increment a small amount for a port with nothing attached.

Examples The following command starts the port statistics monitor beginning with octet statistics (the default):

```
PROMPT# monitor port counters
```

As soon as you press Enter, UNIVERGE WL Control System clears the window and displays statistics at the top of the window.

```
Port  Status          Rx Octets          Tx Octets
=====
  1  Up              27965420          34886544
...
```

To cycle the display to the next set of statistics, press the Spacebar. In this example, packet statistics are displayed next:

```
Port  Status  Rx Unicast  Rx NonUnicast  Tx Unicast  Tx NonUnicast
=====
  1  Up       54620      62144         68318      62556
...
```

Table 4 describes the port statistics displayed by each statistics option. The Port and Status fields are displayed for each option.

Table 4. Output for monitor port counters

Statistics Option	Field	Description
Displayed for All Options	Port	Displays the port statistics.
	Status	Port status. The status can be Up or Down.
octets	Rx Octets	Total number of octets received by the port. This number includes octets received in frames that contained errors.
	Tx Octets	Total number of octets received. This number includes octets received in frames that contained errors.
packets	Rx Unicast	Number of unicast packets received. This number does not include packets that contain errors.
	Rx NonUnicast	Number of broadcast and multicast packets received. This number does not include packets that contain errors.
	Tx Unicast	Number of unicast packets transmitted. This number does not include packets that contain errors.
	Tx NonUnicast	Number of broadcast and multicast packets transmitted. This number does not include packets that contain errors.

Table 4. Output for monitor port counters

Statistics Option	Field	Description
receive-errors	Rx Crc	Number of frames received by the port that had the correct length but contained an invalid frame check sequence (FCS) value. This statistic includes frames with misalignment errors.
	Rx Error	Total number of frames received in which the Physical layer (PHY) detected an error.
	Rx Short	Number of frames received by the port that were fewer than 64 bytes long.
	Rx Overrun	Number of frames received by the port that were valid but were longer than 1518 bytes. This statistic does not include jumbo packets with valid CRCs.
transmit-errors	Tx Crc	Number of frames transmitted by the port that had the correct length but contained an invalid FCS value.
	Tx Short	Number of frames transmitted by the port that were fewer than 64 bytes long.
	Tx Fragment	Total number of frames transmitted that were less than 64 octets long and had invalid CRCs.
	Tx Abort	Total number of frames that had a link pointer parity error.

Table 4. Output for monitor port counters

Statistics Option	Field	Description
collisions	Single Coll	Total number of frames transmitted that experienced one collision before 64 bytes of the frame were transmitted on the network.
	Multiple Coll	Total number of frames transmitted that experienced more than one collision before 64 bytes of the frame were transmitted on the network.
	Excessive Coll	Total number of frames that experienced more than 16 collisions during transmit attempts. These frames are dropped and not transmitted.
	Total Coll	Best estimate of the total number of collisions on this Ethernet segment.
receive-etherstats	Rx 64	Number of packets received that were 64 bytes long.
	Rx 127	Number of packets received that were from 65 through 127 bytes long.
	Rx 255	Number of packets received that were from 128 through 255 bytes long.
	Rx 511	Number of packets received that were from 256 through 511 bytes long.
	Rx 1023	Number of packets received that were from 512 through 1023 bytes long.
	Rx 1518	Number of packets received that were from 1024 through 1518 bytes long.

Table 4. Output for monitor port counters

Statistics Option	Field	Description
transmit-etherstats	Tx 64	Number of packets transmitted that were 64 bytes long.
	Tx 127	Number of packets transmitted that were from 65 through 127 bytes long.
	Tx 255	Number of packets transmitted that were from 128 through 255 bytes long.
	Tx 511	Number of packets transmitted that were from 256 through 511 bytes long.
	Tx 1023	Number of packets transmitted that were from 512 through 1023 bytes long.
	Tx 1518	Number of packets transmitted that were from 1024 through 1518 bytes long.

See Also `show port counters` on page 62

reset port

Resets a port by toggling its link state and Power over Ethernet state.

Syntax `reset port` *port-list*

port-list List of physical ports. UNIVERGE WL Control System resets all the specified ports.

Defaults None.

Access Enabled.

Usage The `reset` command disables the port link for at least 1 second, then reenables them. This behavior is useful for forcing an AP that is connected to two UNIVERGE WL Controller to reboot over the link to the other UNIVERGE WL Controller.

Examples The following command resets port 1:

```
PROMPT# reset port 1
```

See Also **set port** on page 55

set ap

Configures a UNIVERGE WL Access Points, either directly connected to the UNIVERGE WL Controller or indirectly connected through an intermediate Layer 2 or Layer 3 network.



Note. Before configuring a UNIVERGE WL Access Points, you must use the **set system countrycode** command to set the IEEE 802.11 country-specific regulations on the UNIVERGE WL Controller. See **set system countrycode** on page 33.

Syntax **set ap** *ap-number* **serial-id** *serial-ID*
model { **WL1500-AP** | **WL1500-AP-JP** | **WL1700-MS(AP)** } [**radiotype**
 { **11b** | **11g** }]

ap-number

Number for the UNIVERGE WL Access Points.

The range of valid connection numbers depends on the UNIVERGE WL Controller model:

- SCA-WL10—1 to 8 (V1)
- WL5100—1 to 24 (V1)
- WL1700-MS—1 to 8

serial-id *serial-ID*

AP serial ID. The serial ID is listed on the UNIVERGE WL Access Points case. To display the serial ID using the CLI, use the **show version details** command.

model { **WL1500-AP** | **WL1500-AP-JP** | **WL1700-MS(AP)** } AP model.

radiotype **11b** | **11g** Radio type:

- **11b**—802.11b
- **11g**—802.11g

Defaults None.

Access Enabled.

Examples The following command configures UNIVERGE WL Access Points 1 for UNIVERGE WL Access Points model WL1500-AP with serial-ID G8TZUB0053:

```
PROMPT# set ap 1 serial-id G8TZUB0053 model WL1500-AP
success: change accepted.
```

The following command removes UNIVERGE WL Access Points 1:

```
PROMPT# clear ap 1
This will clear specified AP devices. Would you like to continue? (y/n) [n]y
```

See Also

- 1 **clear ap** on page 45
- 1 **monitor port counters** on page 47
- 1 **show port counters** on page 62
- 1 **set system countrycode** on page 33

set port

Administratively disables or reenables a port.

Syntax **set port** {**enable** | **disable**} *port-list*

enable Enables the specified ports.

set port duplex

Chapter 5

disable	Disables the specified ports.
<i>port-list</i>	List of physical ports. UNIVERGE WL Control System disables or reenables all the specified ports.

Defaults All ports are enabled.

Access Enabled.

Usage A port that is administratively disabled cannot send or receive packets. This command does not affect the link state of the port.

Examples The following command disables port 1:

```
PROMPT# set port disable 1
success: set "disable" on port 1
```

The following command reenables the port:

```
PROMPT# set port enable 1
success: set "enable" on port 1
```

See Also **reset port** on page 53

set port duplex

Change the duplex mode of a Ethernet port.

Syntax **set port duplex portlist {full|half}**

<i>port-list</i>	List of physical ports. UNIVERGE WL Control System sets the port duplex mode on all the specified ports.
------------------	--

full	Set the duplex mode of a Ethernet port to full-duplex.
-------------	--

half	Set the duplex mode of a Ethernet port to half-duplex.
-------------	--

Defaults All ports are set to full-duplex.

Access Enabled.

Usage This command is allowed only when a current port speed is 10/100Mbps and current negotiation mode is not autonegotiation. UNIVERGE WL Controller Ethernet ports support half-duplex and full-duplex operation.

Examples The following command sets the port duplex mode on ports 1 to half:

```
PROMPT# set port duplex 1 half
success: set port "1" to half
```

set port name

Assigns a name to a port. After naming a port, you can use the port name or number in other CLI commands.

Syntax **set port** *port name name*

<i>port</i>	Number of a physical port. You can specify only one port.
name <i>name</i>	Alphanumeric string of up to 16 characters, with no spaces.

Defaults None.

Access Enabled.

Usage To simplify configuration and avoid confusion between the number of a port and its name, it is recommended that you do not use numbers as port names.

Examples The following command sets the name of port 1 to *adminpool*:

```
PROMPT# set port 1 name adminpool
success: change accepted.
```

See Also

- 1 **clear port name** on page 47
- 1 **show port status** on page 63

set port negotiation

Disables or reenables autonegotiation on gigabit Ethernet or 10/100 Ethernet ports.

Syntax **set port negotiation** *port-list* { **enable** | **disable** }

port-list List of physical ports. UNIVERGE WL Control System disables or reenables autonegotiation on all the specified ports.

enable Enables autonegotiation on the specified ports.

disable Disables autonegotiation on the specified ports.

Defaults Autonegotiation is enabled on all Ethernet ports by default.

Access Enabled.

Usage UNIVERGE WL Controller Ethernet ports support half-duplex and full-duplex operation.

For a link to occur, the autonegotiation settings on a UNIVERGE WL Controller port and the device at the other end of the link must be the same. When autonegotiation is enabled on a UNIVERGE WL Controller port, the port advertises support for full-duplex and half-duplex mode.

Table 5 lists the supported configurations.

Table 5. Supported 10/100/1000 Ethernet Speeds and Operating Modes for UNIVERGE WL Controllers

UNIVERGE WL Controller Setting		1000 Mbps Full-duplex	100 Mbps Full-duplex	10 Mbps Full-duplex	100 Mbps Half-duplex	10 Mbps Half-duplex	Autonegotiation
Other Device Setting	1000 Mbps Full-duplex	1000 Mbps full-duplex	Not supported	Not supported	Not supported	Not supported	Not supported
	100 Mbps Full-duplex	Not supported	100 Mbps full-duplex	Not supported	Not supported	Not supported	Not supported
	10 Mbps Full-duplex	Not supported	Not supported	10 Mbps full-duplex	Not supported	Not supported	Not supported
	100 Mbps Half-duplex	Not supported	Not supported	Not supported	100 Mbps Half-duplex	Not supported	Not supported
	10 Mbps Half-duplex	Not supported	Not supported	Not supported	Not supported	10 Mbps Half-duplex	Not supported
	Autonegotiation	Not supported	Not supported	Not supported	Not supported	Not supported	1000 Mbps full-duplex

It is recommended that you do not configure the mode of a UNIVERGE WL Controller port so that one side of the link is set to autonegotiation while the other side is set to full-duplex.

Although UNIVERGE WL Control System allows this configuration, it can cause slow throughput on the link.

set port speed

Chapter 5

The slow throughput occurs because the side that is configured for autonegotiation falls back to half-duplex. A stream of large packets sent to a UNIVERGE WL Controller port with this configuration can cause forwarding on the link to stop.

Examples The following command disables autonegotiation on ports 1:

```
PROMPT# set port negotiation 1 disable
```

The following command enables autonegotiation on port 1:

```
PROMPT# set port negotiation 1 enable
```

set port speed

Changes the speed of a port.

Syntax `set port speed port-list { 10 | 100 | 1000 | auto }`

port-list List of physical ports. UNIVERGE WL Control System sets the port speed on all the specified ports.

10 Sets the port speed of a 10/100 Ethernet port to 10 Mbps and sets the operating mode to full-duplex.

100 Sets the port speed of a 10/100 Ethernet port to 100 Mbps and sets the operating mode to full-duplex.

1000 Sets the port speed of a gigabit Ethernet port to 1000 Mbps and sets the operating mode to full-duplex.

Note: This command applies only to the WL5100

auto Enables a port to detect the speed and operating mode of the traffic on the link and set itself accordingly.

Defaults All ports are set to **auto**.

Access Enabled.

Usage It is recommended that you do not configure the mode of a UNIVERGE WL Controller port so that one side of the link is set to autonegotiation while the other side is set to full-duplex. Although UNIVERGE WL Control System allows this configuration, it can result in slow throughput on the link. The slow throughput occurs because the side that is configured for autonegotiation falls back to half-duplex. A stream of large packets sent to a UNIVERGE WL Controller port in such a configuration can cause forwarding on the link to stop.

Do not set the port speed of a gigabit port to auto. Although the CLI allows this setting, it is invalid. If you set the port speed of a gigabit port to auto, the link will stop working.

Examples The following command sets the port speed on ports 1 to 10 Mbps and sets the operating mode to full-duplex:

```
PROMPT# set port speed 1 10
```

set port trap

Enables or disables Simple Network Management Protocol (SNMP) linkup and linkdown traps on an individual port.

Syntax `set port trap port-list {enable | disable}`

<i>port-list</i>	List of physical ports.
enable	Enables the Telnet server.
disable	Disables the Telnet server.

Defaults SNMP linkup and linkdown traps are disabled by default.

Access Enabled.

Usage The **set port trap** command overrides the global setting of the **set snmp notify profile** command. For example, if you globally enable linkup and linkdown traps but then disable the traps on a single port, the **show snmp status** command still indicates that the traps are globally enabled.

Examples The following command enables SNMP linkup and linkdown traps on ports 1:

```
PROMPT# set port trap 1 enable
```

show port counters

Chapter 5

See Also

- 1 **set ip snmp server** on page 122
- 1 **set snmp community** on page 130
- 1 **set snmp usm** on page 146
- 1 **set snmp notify profile** on page 132
- 1 **show snmp community** on page 173

show port counters

Displays port statistics.

Syntax **show port counters** [**octets** | **packets** | **receive-errors** | **transmit-errors** | **collisions** | **receive-etherstats** | **transmit-etherstats**] [**port** *port-list*]

octets	Displays octet statistics.
packets	Displays packet statistics.
receive-errors	Displays errors in received packets.
transmit-errors	Displays errors in transmitted packets.
collisions	Displays collision statistics.
receive-etherstats	Displays Ethernet statistics for received packets.
transmit-etherstats	Displays Ethernet statistics for transmitted packets.
port <i>port-list</i>	List of physical ports. If you do not specify a port list, UNIVERGE WL Control System displays statistics for all ports.

Defaults None.

Access All.

Usage You can specify one statistic type with the command.

Examples The following command shows octet statistics for port 1:

```
PROMPT> show port counters octets port 1
```

Port	Status	Rx Octets	Tx Octets
1	Up	27965420	34886544

This command's output has the same fields as the **monitor port counters** command. For descriptions of the fields, see Table 4 on page 50.

See Also

- 1 **clear port counters** on page 46
- 1 **monitor port counters** on page 47

show port status

Displays configuration and status information for ports.

Syntax **show port status** [*port-list*]

port-list List of physical ports. If you do not specify a port list, information is displayed for all ports.

Defaults None.

Access All.

Examples The following command displays information for ports:

```
PROMPT# show port status
Port Name Admin Oper Config Actual Type Media
=====
1 1 up up auto 100/full network 10/100BaseTx
```

Table 6 describes the fields in this display.

Table 6. Output for show port status

Field	Description
Port	Port number.
Name	Port name. If the port does not have a name, the port number is listed.

Table 6. Output for show port status

Field	Description
Admin	Administrative status of the port: <ul style="list-style-type: none">• up—The port is enabled.• down—The port is disabled.
Oper	Operational status of the port: <ul style="list-style-type: none">• up—The port is operational.• down—The port is not operational.
Config	Port speed configured on the port: <ul style="list-style-type: none">• 10—10 Mbps.• 100—100 Mbps.• 1000—1000 Mbps.• auto—The port sets its own speed.
Actual	Speed and operating mode in effect on the port.
Type	Port type: <ul style="list-style-type: none">• network—Network port
Media	Link type: <ul style="list-style-type: none">• 10/100BaseTX—10/100BASE-T.• 1000BaseT—1000BASE-T.

See Also

1 **set port** on page 55

1 **set port name** on page 57

1 **set port negotiation** on page 58

1 **set port speed** on page 60

VLAN Commands

Use virtual LAN (VLAN) commands to configure and manage parameters for individual port VLANs on network ports, and to display information about clients roaming within a mobility domain. This chapter presents VLAN commands alphabetically. Use the following table to locate commands in this chapter based on their use.

Creation	set vlan name on page 74
Ports	set vlan port on page 75
	clear vlan on page 69
	show vlan config on page 86
Roaming and Tunnels	show roaming station on page 81
	show roaming vlan on page 83
	show tunnel on page 85
Restriction of Client Layer 2 Forwarding	set security l2-restrict on page 73
	show security l2-restrict on page 84
	clear security l2-restrict on page 67
	clear security l2-restrict counters on page 68
Tunnel Affinity	set vlan tunnel-affinity on page 76
FDB Entries	set fdb on page 71
	show fdb on page 77
	show fdb count on page 80
	clear fdb on page 66
FDB Aging Timeout	set fdb agingtime on page 72
	show fdb agingtime on page 79

clear fdb

Deletes an entry from the forwarding database (FDB).

Syntax **clear fdb** { **perm** | **static** | **dynamic** | **port** *port-list* } [**vlan** *vlan-id*] [**tag** *tag-value*]

perm	Clears permanent entries. A permanent entry does not age out and remains in the database even after a reboot, reset, or power cycle. You must specify a VLAN name or number with this option.
static	Clears static entries. A static entry does not age out, but is removed from the database after a reboot, reset, or power cycle. You must specify a VLAN name or number with this option.
dynamic	Clears dynamic entries. A dynamic entry is automatically removed through aging or after a reboot, reset, or power cycle. You are not required to specify a VLAN name or number with this option.
port <i>port-list</i>	Clears dynamic entries that match destination ports in the port list. You are not required to specify a VLAN name or number with this option.
vlan <i>vlan-id</i>	VLAN name or number—required for removing permanent and static entries. For dynamic entries, specifying a VLAN removes entries that match only that VLAN. Otherwise, dynamic entries that match all VLANs are removed.
tag <i>tag-value</i>	VLAN tag value that identifies a virtual port. If you do not specify a tag value, UNIVERGE WL Control System deletes only entries that match untagged interfaces. Specifying a tag value deletes entries that match only the specified tagged interface.

Defaults None.

Access Enabled.

Usage You can delete forwarding database entries based on entry type, port, or VLAN. A VLAN name or number is required for deleting permanent or static entries.

Examples The following command clears all static forwarding database entries that match VLAN *blue*:

```
PROMPT# clear fdb static vlan blue
success: change accepted.
```

The following command clears all dynamic forwarding database entries that match all VLANs:

```
PROMPT# clear fdb dynamic
success: change accepted.
```

The following command clears all dynamic forwarding database entries that match ports 1:

```
PROMPT# clear fdb port 1
success: change accepted.
```

See Also

- 1 **set fdb** on page 71
- 1 **show fdb** on page 77

clear security l2-restrict

Removes one or more MAC addresses from the list of destination MAC addresses that clients in a VLAN are allowed to send traffic at Layer 2.

Syntax **clear security l2-restrict vlan** *vlan-id*
[permit-mac *mac-addr* [*mac-addr*] | **all**]

<i>vlan-id</i>	VLAN name or number.
permit-mac <i>mac-addr</i> [<i>mac-addr</i>]	List of MAC addresses. UNIVERGE WL Control System no longer allows clients in the VLAN to send traffic to the MAC addresses at Layer 2.
all	Removes all MAC addresses from the list.

clear security l2-restrict counters

Chapter 6

Defaults If you do not specify a list of MAC addresses or **all**, all addresses are removed.

Access Enabled.

Usage If you clear all MAC addresses, Layer 2 forwarding is no longer restricted in the VLAN. Clients within the VLAN can communicate directly.

There can be a slight delay before functions such as pinging between clients become available again after Layer 2 restrictions are lifted. Even though packets are passed immediately once Layer 2 restrictions are gone, it can take 10 seconds or more for upper-layer protocols to update their ARP caches and regain their functionality.

To clear the statistics counters without removing any MAC addresses, use the **clear security l2-restrict counters** command instead.

Examples The following command removes MAC address aa:bb:cc:dd:ee:ff from the list of addresses that clients in VLAN *abc_air* are allowed to send traffic at Layer 2:

```
PROMPT# clear security l2-restrict vlan abc_air permit-mac aa:bb:cc:dd:ee:ff
success: change accepted.
```

See Also

- 1 **clear security l2-restrict counters** on page 68
- 1 **set security l2-restrict** on page 73
- 1 **show security l2-restrict** on page 84

clear security l2-restrict counters

Clear statistics counters for Layer 2 forwarding restriction.

Syntax **clear security l2-restrict counters** [**vlan** *vlan-id* | **all**]

vlan-id VLAN name or number.

all Clears Layer 2 forwarding restriction counters for all VLANs.

Defaults If you do not specify a VLAN or **all**, counters for all VLANs are cleared.

Access Enabled.

Usage To clear MAC addresses from the list of addresses that clients are allowed to send data, use the **clear security l2-restrict** command instead.

Examples The following command clears Layer 2 forwarding restriction statistics for VLAN *abc_air*:

```
PROMPT# clear security l2-restrict counters vlan abc_air
success: change accepted.
```

See Also

- 1 **clear security l2-restrict** on page 67
- 1 **set security l2-restrict** on page 73
- 1 **show security l2-restrict** on page 84

clear vlan

Removes physical or virtual ports from a VLAN or removes a VLAN entirely.



Caution! When you remove a VLAN, UNIVERGE WL Control System completely removes the VLAN from the configuration and also removes all configuration information that uses the VLAN. If you want to remove only a specific port from the VLAN, make sure you specify the port number in the command.

Syntax **clear vlan** *vlan-id* [**port** *port-list* [**tag** *tag-value*]]

vlan-id VLAN name or number.

port <i>port-list</i>	List of physical ports. UNIVERGE WL Control System removes the specified ports from the VLAN. If you do not specify a list of ports, UNIVERGE WL Control System removes the VLAN entirely.
tag <i>tag-value</i>	Tag number that identifies a virtual port. UNIVERGE WL Control System removes only the specified virtual port from the specified physical ports.

Defaults None.

Access Enabled.

Usage If you do not specify a *port-list*, the entire VLAN is removed from the configuration.



Note. You cannot delete the default VLAN but you can remove ports from it. To remove ports from the default VLAN, use the **port** *port-list* option.

Examples The following command removes port 1 from VLAN *green*:

```
PROMPT# clear vlan green port 1
This may disrupt user connectivity. Do you wish to continue? (y/n) [n]y
success: change accepted.
```

The following command removes port 1, which uses tag value 69, from VLAN *red*:

```
PROMPT# clear vlan red port 1 tag 69
This may disrupt user connectivity. Do you wish to continue? (y/n) [n]y
success: change accepted.
```

The following command completely removes VLAN *marigold*:

```
PROMPT# clear vlan marigold
This may disrupt user connectivity. Do you wish to continue? (y/n) [n]y
success: change accepted.
```

See Also

- 1 **set vlan port** on page 75
- 1 **show vlan config** on page 86

set fdb

Adds a permanent or static entry to the forwarding database.

Syntax **set fdb** {**perm** | **static**} *mac-addr* **port** *port-list*
vlan *vlan-id* [**tag** *tag-value*]

perm	Adds a permanent entry. A permanent entry does not age out and remains in the database even after a reboot, reset, or power cycle.
static	Adds a static entry. A static entry does not age out, but is removed from the database after a reboot, reset, or power cycle.
<i>mac-addr</i>	Destination MAC address of the entry. Use colons to separate the octets (for example, 00:11:22:aa:bb:cc).
port <i>port-list</i>	List of physical destination ports for which to add the entry.
vlan <i>vlan-id</i>	Name or number of a VLAN of which the port is a member. The entry is added only for the specified VLAN.
tag <i>tag-value</i>	VLAN tag value that identifies a virtual port. You can specify a number from 1 through 4093. If you do not specify a tag value, an entry is created for an untagged interface only. If you specify a tag value, an entry is created only for the specified tagged interface.

Defaults None.

Access Enabled.

Usage You cannot add a multicast or broadcast address as a permanent or static FDB entry.

Examples The following command adds a permanent entry for MAC address 00:11:22:aa:bb:cc on ports 1 in VLAN *blue*:

```
PROMPT# set fdb perm 00:11:22:aa:bb:cc port 1 vlan blue
success: change accepted.
```

set fdb agingtime

Chapter 6

The following command adds a static entry for MAC address 00:2b:3c:4d:5e:6f on port 1 in the *default* VLAN:

```
PROMPT# set fdb static 00:2b:3c:4d:5e:6f port 1 vlan default
success: change accepted.
```

See Also

1 **clear fdb** on page 66

1 **show fdb** on page 77

set fdb agingtime

Changes the aging timeout period for dynamic entries in the forwarding database.

Syntax **set fdb agingtime** *vlan-id* **age** *seconds*

vlan-id VLAN name or number. The timeout period change applies only to entries that match the specified VLAN.

age *seconds* Value for the timeout period, in seconds. You can specify a value from 0 through 1,000,000. If you change the timeout period to 0, aging is disabled.

Defaults The aging timeout period is 300 seconds (5 minutes).

Access Enabled.

Examples The following command changes the aging timeout period to 600 seconds for entries that match VLAN *orange*:

```
PROMPT# set fdb agingtime orange age 600
success: change accepted.
```

See Also **show fdb agingtime** on page 79

set security l2-restrict

Restricts Layer 2 forwarding between clients in the same VLAN. When you restrict Layer 2 forwarding in a VLAN, UNIVERGE WL Control System allows Layer 2 forwarding only between a client and a set of MAC addresses, generally the VLAN default routers. Clients within the VLAN are not permitted to communicate among themselves directly. To communicate with another client, the client must use one of the specified default routers.

Syntax `set security l2-restrict vlan vlan-id`
`[mode {enable | disable}] [permit-mac mac-addr [mac-addr]]`

<i>vlan-id</i>	VLAN name or number.
mode {enable disable}	Enables or disables restriction of Layer 2 forwarding.
permit-mac <i>mac-addr</i> [<i>mac-addr</i>]	MAC addresses to which clients are allowed to forward data at Layer 2. You can specify up to four addresses.

Defaults Layer 2 restriction is disabled by default.

Access Enabled.

Usage You can specify multiple addresses by listing them on the same command line or by entering multiple commands. To change a MAC address, use the **clear security l2-restrict** command to remove it, and then use the **set security l2-restrict** command to add the correct address.

Restriction of client traffic does not begin until you enable the permitted MAC list. Use the **mode enable** option with this command.

Examples The following command restricts Layer 2 forwarding of client data in VLAN *abc_air* to the default routers with MAC address aa:bb:cc:dd:ee:ff and 11:22:33:44:55:66:

```
PROMPT# set security l2-restrict vlan abc_air mode enable permit-mac
aa:bb:cc:dd:ee:ff 11:22:33:44:55:66
success: change accepted.
```

See Also

- 1 **clear security l2-restrict** on page 67
- 1 **clear security l2-restrict counters** on page 68
- 1 **show security l2-restrict** on page 84

set vlan name

Creates a VLAN and assigns a number and name to it.

Syntax **set vlan** *vlan-num* **name** *name*

vlan-num VLAN number. You can specify a number from 2 through 4093.

name String up to 16 alphabetic characters long.

Defaults VLAN 1 is named *default* by default. No other VLANs have default names.

Access Enabled.

Usage You must assign a name to a VLAN (other than the default VLAN) before you can add ports to the VLAN.

It is recommended that you do not use the name *default*. This name is already used for VLAN 1. It is also recommended that you do not rename the default VLAN.

You cannot use a number as the first character in the VLAN name. It is recommended that you do not use the same name with different capitalizations for VLANs. For example, do not configure two separate VLANs with the names *red* and *RED*.

VLAN names are case-sensitive for RADIUS authorization when a client roams to a UNIVERGE WL Controller. If the UNIVERGE WL Controller is not configured with the VLAN of the client, but is configured with a VLAN with the same spelling but different capitalization, authorization for the client fails. For example, if the client is on VLAN *red* but the UNIVERGE WL Controller to which the client roams has VLAN *RED* instead, RADIUS authorization fails.

Examples The following command assigns the name *marigold* to VLAN 3:

```
PROMPT# set vlan 3 name marigold
success: change accepted.
```

See Also **set vlan port** on page 75

set vlan port

Assigns one or more network ports to a VLAN. You also can add a virtual port to each network port by adding a tag value to the network port.

Syntax **set vlan** *vlan-id* **port** *port-list* [**tag** *tag-value*]

vlan-id VLAN name or number.

port *port-list* List of physical ports.

tag *tag-value* Tag value that identifies a virtual port. You can specify a value from 1 through 4093.

Defaults By default, no ports are members of any VLANs. A UNIVERGE WL Controller cannot forward traffic on the network until you configure VLANs and add network ports to the VLANs.

Access Enabled.

Usage You can combine this command with the **set port name** command to assign the name and add the ports at the same time.

If you do not specify a tag value, the UNIVERGE WL Controller sends untagged frames for the VLAN. If you do specify a tag value, the UNIVERGE WL Controller sends tagged frames only for the VLAN.

If you do specify a tag value, it is recommended to use the same value as the VLAN number. UNIVERGE WL Control System does not require the VLAN number and tag value to be the same but it can be required by devices from other vendors.

Examples The following command assigns the name *beige* to VLAN 11 and adds ports 1 through 3 to the VLAN:

```
PROMPT# set vlan 11 name beige port 1-3
success: change accepted.
```

set vlan tunnel-affinity

Chapter 6

The following command adds port 16 to VLAN *beige* and assigns tag value 86 to the port:

```
PROMPT# set vlan beige port 16 tag 86
success: change accepted.
```

See Also

- 1 **clear vlan** on page 69
- 1 **set vlan name** on page 74
- 1 **show vlan config** on page 86

set vlan tunnel-affinity

Changes a UNIVERGE WL Controller preferences within a mobility domain for tunneling user traffic for a VLAN. When a user roams to a UNIVERGE WL Controller that is not a member of the user's VLAN, the UNIVERGE WL Controller can forward the user traffic by tunneling to another UNIVERGE WL Controller that is a member of the VLAN.

Syntax **set vlan** *vlan-id* **tunnel-affinity** *num*

vlan-id VLAN name or number.

num Preference of this UNIVERGE WL Controller for forwarding user traffic for the VLAN. You can specify a value from 1 through 10. A higher number indicates a greater preference.

Defaults Each VLAN on a UNIVERGE WL Controller network ports has an affinity value of 5 by default.

Access Enabled.

Usage Increasing a UNIVERGE WL Controller affinity value increases the preferability of the UNIVERGE WL Controller for forwarding user traffic for the VLAN.

If more than one UNIVERGE WL Controller has the highest affinity value, UNIVERGE WL Control System randomly selects one of the UNIVERGE WL Controllers for the tunnel.

Examples The following command changes the VLAN affinity for VLAN *beige* to 10:

```
PROMPT# set vlan beige tunnel-affinity 10
success: change accepted.
```

See Also

- 1 **show roaming vlan** on page 83
- 1 **show vlan config** on page 86

show fdb

Displays entries in the forwarding database.

Syntax **show fdb** [*mac-addr-glob* [**vlan** *vlan-id*]]

show fdb { **permanent** | **static** | **dynamic** | **system** | **all** } [**port** *port-list* | **vlan** *vlan-id*]

<i>mac-addr-glob</i>	A single MAC address or set of MAC addresses. Specify a MAC address, or use the wildcard character (*) to specify a set of MAC addresses. (For details, see “MAC Address Globs” on page 10.)
vlan <i>vlan-id</i>	Name or number of a VLAN for which to display entries.
permanent	Displays permanent entries. A permanent entry does not age out and remains in the database even after a reboot, reset, or power cycle.
static	Displays static entries. A static entry does not age out, but is removed from the database after a reboot, reset, or power cycle.
dynamic	Displays dynamic entries. A dynamic entry is automatically removed through aging or after a reboot, reset, or power cycle.

show fdb

Chapter 6

system	Displays system entries. A system entry is added by UNIVERGE WL Control System. For example, the authentication protocols can add entries for wired and wireless authentication users.
all	Displays all entries in the database, or all the entries that match a particular port or ports or a particular VLAN.
port <i>port-list</i>	Destination port(s) for which to display entries.

Defaults None.

Access All.

Usage To display the entire forwarding database, enter the **show fdb** command without options. To display only a portion of the database, use optional parameters to specify the types of entries you want to display.

Examples The following command displays all entries in the forwarding database:

```
PROMPT# show fdb all
* = Static Entry. + = Permanent Entry. # = System Entry.
VLAN TAG  Dest MAC/Route Des [CoS] Destination Ports [Protocol Type]
-----
1         00:01:97:13:0b:1f          1          [ALL]
1         aa:bb:cc:dd:ee:ff          *          3          [ALL]
1         00:0b:0e:02:76:f5          1          [ALL]
Total Matching FDB Entries Displayed = 3
```

The top line of the display identifies the characters to distinguish among the entry types.

The following command displays all entries that begin with the MAC address glob 00:

```
PROMPT# show fdb 00:*
* = Static Entry. + = Permanent Entry. # = System Entry.
VLAN TAG  Dest MAC/Route Des [CoS] Destination Ports [Protocol Type]
-----
1         00:01:97:13:0b:1f          1          [ALL]
1         00:0b:0e:02:76:f5          1          [ALL]
Total Matching FDB Entries Displayed = 2
```

Table 7 describes the fields in the **show fdb** output.

Table 7. Output for show fdb

Field	Description
VLAN	VLAN number.
TAG	VLAN tag value. If the interface is untagged, the TAG field is blank.
Dest MAC/Route Des	MAC address of the forwarding entry destination.
CoS	Type of entry. The entry types are explained in the first row of the command output. Note: This Class of Service (CoS) value is not associated with UNIVERGE WL Control System quality of service (QoS) features.
Destination Ports	UNIVERGE WL Controller port associated with the entry. A UNIVERGE WL Controller sends traffic to the destination MAC address through this port.
Protocol Type	Layer 3 protocol address types that can be mapped to this entry.
Total Matching FDB Entries Displayed	Number of entries displayed by the command.

See Also

1 **clear fdb** on page 66

1 **set fdb** on page 71

show fdb agingtime

Displays the aging timeout period for forwarding database entries.

Syntax **show fdb agingtime** [**vlan** *vlan-id*]

vlan *vlan-id* VLAN name or number. If you do not specify a VLAN, the aging timeout period for each VLAN is displayed.

show fdb count

Chapter 6

Defaults None.

Access All.

Examples The following command displays the aging timeout period for all VLANs:

```
PROMPT# show fdb agingtime
VLAN 2 aging time = 600 sec
VLAN 1 aging time = 300 sec
```

Because the forwarding database aging timeout period can be configured only on an individual VLAN basis, the command lists the aging timeout period for each VLAN separately.

See Also **set fdb agingtime** on page 72

show fdb count

Lists the number of entries in the forwarding database.

Syntax **show fdb count** {**permanent** | **static** | **dynamic**} [**vlan** *vlan-id*]

permanent	Lists the number of permanent entries. A permanent entry does not age out and remains in the database even after a reboot, reset, or power cycle.
static	Lists the number of static entries. A static entry does not age out, but is removed from the database after a reboot, reset, or power cycle.
dynamic	Lists the number of dynamic entries. A dynamic entry is automatically removed through aging or after a reboot, reset, or power cycle.
vlan <i>vlan-id</i>	VLAN name or number. Entries are listed for only the specified VLAN.

Defaults None.

Access All.

Examples The following command lists the number of dynamic entries that the forwarding database contains:

```
PROMPT# show fdb count dynamic
Total Matching Entries = 2
```

See Also **show fdb** on page 77

show roaming station

Displays a list of the stations roaming to the UNIVERGE WL Controller through a VLAN tunnel.

Syntax **show roaming station** [**vlan** *vlan-id*] [**peer** *ip-addr*]

vlan *vlan-id* Output is restricted to stations using this VLAN.

peer *ip-addr* Output is restricted to stations tunnelling through this peer UNIVERGE WL Controller in the Mobility Domain.

Defaults None.

Access Enabled.

Usage The output displays roaming stations within the previous 1 second.

Examples To display all stations roaming to the UNIVERGE WL Controller, type the following command:

```
PROMPT# show roaming station
User Name      Station Address  VLAN      State
-----
redsqa         10.10.10.5       violet     Up
```

show roaming station

Chapter 6

Table 8 describes the fields in the display.

Table 8. Output for show roaming station

Field	Description
User Name	Name of the user. This is the name used for authentication. The name resides in a RADIUS server database or the local user database on a UNIVERGE WL Controller.
Station Address	IP address of the user device.
VLAN	Name of the VLAN that the RADIUS server or UNIVERGE WL Controller local user database assigned the user.
State	<p>State of the session:</p> <ul style="list-style-type: none">• Setup—Station is attempting to roam to this UNIVERGE WL Controller. This UNIVERGE WL Controller has asked the UNIVERGE WL Controller from which the station is roaming for the station session information and is waiting for a reply.• Up—UNIVERGE WL Control System has established a tunnel between the UNIVERGE WL Controllers and the station has successfully roamed to this UNIVERGE WL Controller over the tunnel.• Chck—This UNIVERGE WL Controller is in the process of accepting a reassociation request from the roaming peer UNIVERGE WL Controller for a station currently roaming to the peer UNIVERGE WL Controller.• TChck—This UNIVERGE WL Controller is in the process of accepting a reassociation request from the roaming peer UNIVERGE WL Controller for a station currently roaming to this UNIVERGE WL Controller.• WInd—This UNIVERGE WL Controller is waiting for network congestion to clear before sending the roaming indication to the roaming peer UNIVERGE WL Controller.• WResp—This UNIVERGE WL Controller is waiting for network congestion to clear before sending the roaming response to the roaming peer UNIVERGE WL Controller.

See Also `show roaming vlan` on page 83

show roaming vlan

Shows all VLANs in the mobility domain, the UNIVERGE WL Controllers servicing the VLANs, and their tunnel affinity values configured on each UNIVERGE WL Controller for the VLANs.

Syntax `show roaming vlan`

Defaults None.

Access Enabled.

Examples The following command shows the current roaming VLANs:

```
PROMPT# show roaming vlan
VLAN          Switch IP Address  Affinity
-----
vlan-cs        192.168.14.2        5
vlan-eng        192.168.14.4        5
vlan-fin        192.168.14.2        5
vlan-it         192.168.14.4        5
vlan-it         192.168.14.2        5
vlan-pm         192.168.14.2        5
vlan-sm         192.168.14.2        5
vlan-tp         192.168.14.4        5
vlan-tp         192.168.14.2        5
```

Table 9 describes the fields in the display.

Table 9. Output for show roaming vlan

Field	Description
VLAN	VLAN name.
Switch IP Address	System IP address of the UNIVERGE WL Controller on which the VLAN is configured.
Affinity	Preference of this UNIVERGE WL Controller for forwarding user traffic for the VLAN. A higher number indicates a greater preference.

See Also

- 1 **show roaming station** on page 81
- 1 **show vlan config** on page 86

show security l2-restrict

Displays configuration information and statistics for Layer 2 forwarding restriction.

Syntax **show security l2-restrict** [**vlan** *vlan-id* | **all**]

vlan-id VLAN name or number.

all Displays information for all VLANs.

Defaults If you do not specify a VLAN name or **all**, information is displayed for all VLANs.

Access Enabled.

Examples The following command shows Layer 2 forwarding restriction information for all VLANs:

```
PROMPT# show security l2-restrict
VLAN Name          En Drops      Permit MAC          Hits
-----
  1 default          Y              0 00:60:b9:11:53:3e  5947
                    00:60:b9:11:5c:a8    9
  2 vlan-2           Y              0 04:04:04:04:04:04    0
```

Table 10 describes the fields in the display.

Table 10. Output for show security l2-restrict

Field	Description
VLAN	VLAN number.
Name	VLAN name.
En	Enabled state of the feature for the VLAN: <ul style="list-style-type: none"> Y—Enabled. Forwarding of Layer 2 traffic from clients is restricted to the MAC address(es) listed under Permit MAC. N—Disabled. Layer 2 forwarding is not restricted.
Drops	Number of packets dropped because the destination MAC address is not one of the addresses listed under Permit MAC.

Table 10. Output for show security l2-restrict

Field	Description
Permit MAC	MAC addresses that clients in the VLAN are allowed to send traffic at Layer 2.
Hits	Number of packets whose source MAC address was a client in this VLAN, and whose destination MAC address was one of those listed under Permit MAC.

See Also

- 1 **clear security l2-restrict** on page 67
- 1 **clear security l2-restrict counters** on page 68
- 1 **set security l2-restrict** on page 73

show tunnel

Displays the tunnels from the UNIVERGE WL Controller where you type the command.

Syntax **show tunnel**

Defaults None.

Access Enabled

Examples To display all tunnels from a UNIVERGE WL Controller to other UNIVERGE WL Controllers in the Mobility Domain, type the following command.

```
PROMPT# show tunnel
VLAN      Local Address  Remote Address  State    Port  LVID  RVID
-----
vlan-eng   192.168.14.2    192.168.14.4   DORMANT  1024  4096  130
```

Table 11 describes the fields in the display.

Table 11. Output for show tunnel

Field	Description
VLAN	VLAN name.
Local Address	IP address of the local end of the tunnel. This is the UNIVERGE WL Controller IP address where you enter the command.
Remote Address	IP address of the remote end of the tunnel. This is the system IP address of another UNIVERGE WL Controller in the mobility domain.
State	Tunnel state: <ul style="list-style-type: none">• Up• Dormant
Port	Tunnel port ID.
LVID	Local VLAN ID.
RVID	Remote VLAN ID.

See Also **show vlan config** on page 86

show vlan config

Displays VLAN information.

Syntax **show vlan config** [*vlan-id*]

vlan-id VLAN name or number. If you do not specify a VLAN, information for all VLANs is displayed.

Defaults None.

Access All.

Examples The following command displays information for VLAN *burgundy*:

```
PROMPT# show vlan config burgundy
```

VLAN	Name	Admin Status	VLAN State	Tunl Affin	Port	Tag	Port State
2	burgundy	Up	Up		5		
					2	none	Up
					3	none	Up
					4	none	Up
					6	none	Up
					11	none	Up
					t:10.10.40.4	none	Up

Table 12 describes the fields in this display.

Table 12. Output for show vlan config

Field	Description
VLAN	VLAN number.
Name	VLAN name.
Admin Status	Administrative status of the VLAN: <ul style="list-style-type: none"> Down—The VLAN is disabled. Up—The VLAN is enabled.
VLAN State	Link status of the VLAN: <ul style="list-style-type: none"> Down—The VLAN is not connected. Up—The VLAN is connected.
Tunl Affin	Tunnel affinity value assigned to the VLAN.
Port	Member port of the VLAN. The port can be a physical port or a virtual port. <ul style="list-style-type: none"> Physical ports are 10/100 Ethernet or gigabit Ethernet ports on the UNIVERGE WL Controller, and are listed by port number. Virtual ports are tunnels to other UNIVERGE WL Controllers in a mobility domain, and are listed as follows: t:<i>ip-addr</i>, where <i>ip-addr</i> is the system IP address of the UNIVERGE WL Controller at the other end of the tunnel.

Table 12. Output for show vlan config

Field	Description
Tag	Tag value assigned to the port.
Port State	Link state of the port: <ul style="list-style-type: none">• Down—The port is not connected.• Up—The port is connected.

See Also

- 1 **clear vlan** on page 69
- 1 **set vlan name** on page 74
- 1 **set vlan port** on page 75
- 1 **set vlan tunnel-affinity** on page 76

Quality of Service Commands

Use Quality of Service (QoS) commands to configure packet prioritization in UNIVERGE WL Control System. Packet prioritization ensures that UNIVERGE WL Controllers and UNIVERGE WL Access Points give preferential treatment to high-priority traffic such as voice and video.

(To override the prioritization for specific traffic, use access controls lists [ACLs] to set the Class of Service [CoS] for the packets. See Chapter 14, “Security ACL Commands,” on page 453.)

This chapter presents QoS commands alphabetically. Use the following table to locate commands in this chapter based on their use.

QoS Settings

show qos on page 92

show qos dscp-table on page 93

set qos cos-to-dscp-map on page 91

set qos dscp-to-cos-map on page 91

clear qos on page 90

clear qos

Resets the UNIVERGE WL Controller mapping of Differentiated Services Code Point (DSCP) values to internal QoS values.

The UNIVERGE WL Controller internal QoS map ensures that prioritized traffic remains prioritized while transiting the UNIVERGE WL Controller. A UNIVERGE WL Controller uses the QoS map to do the following:

- 1 Classify inbound packets by mapping their DSCP values to one of eight internal QoS values
- 1 Classify outbound packets by marking their DSCP values based on the UNIVERGE WL Controllers internal QoS values

Syntax **clear qos**

[cos-to-dscp-map [from-qos] | dscp-to-cos-map [from-dscp]]

cos-to-dscp-map
[from-qos]

Resets the mapping between the specified internal QoS value and the DSCP values with which UNIVERGE WL Control System marks outbound packets. QoS values are from 0 to 7.

dscp-to-cos-map
[from-dscp]

Resets the mapping between the specified range of DSCP values and internal QoS value with which UNIVERGE WL Control System classifies inbound packets.

Defaults None.

Access Enabled.

Usage To reset all mappings to their default values, use the **clear qos** command without the optional parameters.

Examples The following command resets all QoS mappings:

```
PROPMT# clear qos
success: change accepted.
```

The following command resets the mapping used to classify packets with DSCP value 44:

```
PROPMT# clear qos dscp-to-qos-map 44
success: change accepted.
```

set qos cos-to-dscp-map

Changes the value that UNIVERGE WL Control System maps an internal QoS value when marking outbound packets.

Syntax `set qos cos-to-dscp-map level dscp dscp-value`

level Internal CoS value. You can specify a number from 0 to 7.

dscp *dscp-value* DSCP value. You can specify the value as a decimal number. Valid values are 0 to 63.

Defaults The defaults are listed by the **show qos** command.

Access Enabled.

Examples The following command maps internal CoS value 5 to DSCP value 50:

```
PROPMT# set qos cos-to-dscp-map 5 dscp 50
warning: cos 5 is marked with dscp 50 which will be classified as cos 6
```

If the change results in a change to CoS, UNIVERGE WL Control System displays a warning message indicating the change. In this example, packets receiving CoS 5 upon ingress are marked with a DSCP value equivalent to CoS 6 upon egress.

See Also

1 **set qos dscp-to-cos-map** on page 91

1 **show qos** on page 92

set qos dscp-to-cos-map

Changes the internal QoS value that UNIVERGE WL Control System maps to a packet DSCP value when classifying inbound packets.

Syntax `set qos dscp-to-cos-map dscp-range cos level`

<i>dscp-range</i>	DSCP range. You can specify the values as decimal numbers. Valid decimal values are 0 to 63. To specify a range, use the following format: 40-56. Specify the lower number first.
<i>cos level</i>	Internal QoS value. You can specify a number from 0 to 7.

Defaults The defaults are listed by the **show qos** command.

Access Enabled.

Examples The following command maps DSCP values 40-56 to internal CoS value 6:

```
PROPMT# set qos dscp-to-cos-map 40-56 cos 6
warning: cos 5 is marked with dscp 63 which will be classified as cos 7
warning: cos 7 is marked with dscp 56 which will be classified as cos 6
```

As shown in this example, if the change results in a change to CoS, UNIVERGE WL Control System displays a warning message indicating the change.

See Also

1 **set qos cos-to-dscp-map** on page 91

1 **show qos** on page 92

show qos

Displays the UNIVERGE WL Controller QoS settings.

Syntax `show qos [default]`

default	Displays the default mappings.
----------------	--------------------------------

Defaults None.

Access Enabled.

Examples The following command displays the default QoS settings:

PROPMT# **show qos default**

Ingress QoS Classification Map (dscp-to-cos)

Ingress DSCP	CoS Level									
00-09	0	0	0	0	0	0	0	0	1	1
10-19	1	1	1	1	1	1	2	2	2	2
20-29	2	2	2	2	3	3	3	3	3	3
30-39	3	3	4	4	4	4	4	4	4	4
40-49	5	5	5	5	5	5	5	5	6	6
50-59	6	6	6	6	6	6	7	7	7	7
60-63	7	7	7	7						

Egress QoS Marking Map (cos-to-dscp)

CoS Level	0	1	2	3	4	5	6	7
=====								
Egress DSCP	0	8	16	24	32	40	48	56
Egress ToS byte	0x00	0x20	0x40	0x60	0x80	0xA0	0xC0	0xE0

See Also **show qos dscp-table** on page 93

show qos dscp-table

Displays a table that maps Differentiated Services Code Point (DSCP) values to their equivalent combinations of IP precedence values and IP ToS values.

Syntax **show qos dscp-table**

Defaults None.

Access Enabled.

Examples The following command displays the table:

PROPMT# **show qos dscp-table**

DSCP		TOS		precedence	tos
dec	hex	dec	hex		

0	0x00	0	0x00	0	0
1	0x01	4	0x04	0	2
2	0x02	8	0x08	0	4
...					
63	0x3f	252	0xfc	7	14

show qos dscp-table

Chapter 7

See Also **show qos** on page 92

IP Services Commands

Use IP services commands to configure and manage IP interfaces, management services, the Domain Name Service (DNS), Network Time Protocol (NTP), aliases, and to ping a host or trace a route. This chapter presents IP services commands alphabetically. Use the following table to locate commands in this chapter based on their use.

IP Interface	set interface on page 111
	set interface dhcp-client on page 112
	set interface status on page 115
	show interface on page 161
	show dhcp-client on page 157
	clear interface on page 97
System IP Address	set system ip-address on page 153
	clear system ip-address on page 106
IP Route	set ip route on page 120
	show ip route on page 167
	clear ip route on page 100
SSH Management	set ip ssh server on page 124
	set ip ssh on page 123
Telnet Management	set ip telnet on page 125
	set ip telnet server on page 126
	show ip telnet on page 169
	clear ip telnet on page 101
HTTPS Management	set ip https server on page 119
	show ip https on page 165

DNS

set ip dns on page 116
set ip dns domain on page 117
set ip dns server on page 118
show ip dns on page 164
clear ip dns domain on page 99
clear ip dns server on page 99

IP Alias

set ip alias on page 115
show ip alias on page 163
clear ip alias on page 98

Time and Date

set time date on page 154
set timezone on page 155
set summertime on page 151
show time date on page 176
show timezone on page 177
show summertime on page 175
clear timezone on page 107
clear summertime on page 105

NTP

set ntp on page 127
set ntp server on page 128
set ntp update-interval on page 129
show ntp on page 170
clear ntp server on page 102
clear ntp update-interval on page 102

ARP

set arp on page 109
set arp agingtime on page 110
show arp on page 156

SNMP

set snmp protocol on page 143
set snmp security on page 144
set snmp community on page 130

	set snmp usm on page 146
	set snmp notify profile on page 132
	set snmp notify target on page 137
	set ip snmp server on page 122
	show snmp status on page 174
	show snmp community on page 173
	show snmp usm on page 175
	show snmp notify profile on page 173
	show snmp notify target on page 174
	show snmp counters on page 173
	clear snmp community on page 103
	clear snmp usm on page 105
	clear snmp notify profile on page 103
	clear snmp notify target on page 104
Ping	ping on page 107
Telnet client	telnet on page 177
Traceroute	traceroute on page 179
DHCP server	set interface dhcp-server on page 113
	show dhcp-server on page 159

clear interface

Removes an IP interface.

Syntax **clear interface** *vlan-id* **ip**

vlan-id VLAN name or number.

Defaults None.

Access Enabled.

clear ip alias

Chapter 8

Usage If the interface you want to remove is configured as the system IP address, removing the address can interfere with system tasks using the system IP address, including the following:

- 1 Mobility domain operations
- 1 Topology reporting for dual-homed AP
- 1 Default source IP address used in unsolicited communications such as AAA accounting reports and SNMP traps

Examples The following command removes the IP interface configured on VLAN *mauve*:

```
PROMPT# clear interface mauve ip
success: cleared ip on vlan mauve
```

See Also

- 1 **set interface** on page 111
- 1 **set interface status** on page 115
- 1 **show interface** on page 161

clear ip alias

Removes an alias, which is a string that represents an IP address.

Syntax `clear ip alias name`

name Alias name.

Defaults None.

Access Enabled.

Examples The following command removes the alias *server1*:

```
PROMPT# clear ip alias server1
success: change accepted.
```

See Also

- 1 **set ip alias** on page 115

- 1 **show ip alias** on page 163

clear ip dns domain

Removes the default DNS domain name.

Syntax **clear ip dns domain**

Defaults None.

Access Enabled.

Examples The following command removes the default DNS domain name from a UNIVERGE WL Controller:

```
PROMPT# clear ip dns domain
Default DNS domain name cleared.
```

See Also

- 1 **clear ip dns server** on page 99
- 1 **set ip dns** on page 116
- 1 **set ip dns domain** on page 117
- 1 **set ip dns server** on page 118
- 1 **show ip dns** on page 164

clear ip dns server

Removes a DNS server from a UNIVERGE WL Controller configuration.

Syntax **clear ip dns server** *ip-addr*

ip-addr IP address of a DNS server.

Defaults None.

Access Enabled.

clear ip route

Chapter 8

Examples The following command removes DNS server 10.10.10.69 from a UNIVERGE WL Controller configuration:

```
PROMPT# clear ip dns server 10.10.10.69
success: change accepted.
```

See Also

- 1 **clear ip dns domain** on page 99
- 1 **set ip dns** on page 116
- 1 **set ip dns domain** on page 117
- 1 **set ip dns server** on page 118
- 1 **show ip dns** on page 164

clear ip route

Removes a route from the IP route table.

Syntax **clear ip route** {**default** | *ip-addr mask* | *ip-addr/mask-length*}
default-router

default	Default route.
	Note: default is an alias for IP address 0.0.0.0/0.
<i>ip-addr mask</i>	IP address and subnet mask for the route destination, in dotted decimal notation (for example, 10.10.10.10 255.255.255.0).
<i>ip-addr/mask-length</i>	IP address and subnet mask length in CIDR format (for example, 10.10.10.10/24).
<i>default-router</i>	IP address, DNS hostname, or alias of the next-hop router.

Defaults None.

Access Enabled.

Examples The following command removes the route to destination 10.10.10.68/24 through router 10.10.10.1:

```
PROMPT# clear ip route 10.10.10.68/24 10.10.10.1
success: change accepted.
```

See Also

- 1 **set ip route** on page 120
- 1 **show ip route** on page 167

clear ip telnet

Resets the Telnet server TCP port number to its default value. A UNIVERGE WL Controller listens for Telnet management traffic on the Telnet server port.

Syntax **clear ip telnet**

Defaults The default Telnet port number is 23.

Access Enabled.

Examples The following command resets the TCP port number for Telnet management traffic to its default:

```
PROMPT# clear ip telnet
success: change accepted.
```

See Also

- 1 **set ip https server** on page 119
- 1 **set ip telnet** on page 125
- 1 **set ip telnet server** on page 126
- 1 **show ip https** on page 165
- 1 **show ip telnet** on page 169

clear ntp server

Removes an NTP server from a UNIVERGE WL Controller configuration.

Syntax **clear ntp server** {*ip-addr* | **all**}

ip-addr IP address of the server to remove, in dotted decimal notation.

all Removes all NTP servers from the configuration.

Defaults None.

Access Enabled.

Examples The following command removes NTP server 192.168.40.240 from a UNIVERGE WL Controller configuration:

```
PROMPT# clear ntp server 192.168.40.240
success: change accepted.
```

See Also

- 1 **clear ntp update-interval** on page 102
- 1 **set ntp** on page 127
- 1 **set ntp server** on page 128
- 1 **set ntp update-interval** on page 129
- 1 **show ntp** on page 170

clear ntp update-interval

Resets the NTP update interval to the default value.

Syntax **clear ntp update-interval**

Defaults The default NTP update interval is 64 seconds.

Access Enabled.

Examples To reset the NTP interval to the default value, type the following command:

```
PROMPT# clear ntp update-interval
success: change accepted.
```

See Also

- 1 **clear ntp server** on page 102
- 1 **set ntp** on page 127
- 1 **set ntp server** on page 128
- 1 **set ntp update-interval** on page 129
- 1 **show ntp** on page 170

clear snmp community

Clears an SNMP community string.

Syntax **clear snmp community name** *comm-string*

comm-string Name of the SNMP community you want to clear.

Defaults None.

Access Enabled.

Examples The following command clears community string *setswitch2*:

```
PROMPT# clear snmp community name setswitch2
success: change accepted.
```

See Also

- 1 **set snmp community** on page 130
- 1 **show snmp community** on page 173

clear snmp notify profile

Clears an SNMP notification profile.

clear snmp notify target

Chapter 8

Syntax **clear snmp notify profile** *profile-name*

profile-name Name of the notification profile you are clearing.

Defaults None.

Access Enabled.

Examples The following command clears notification profile *snmpprof_rfdetect*:

```
PROMPT# clear snmp notify profile snmpprof_rfdetect
success: change accepted.
```

See Also

- 1 **set snmp notify profile** on page 132
- 1 **show snmp notify profile** on page 173

clear snmp notify target

Clears an SNMP notification target.

Syntax **clear snmp notify target** *target-num*

target-num ID of the target.

Defaults None.

Access Enabled.

Examples The following command clears notification target 3:

```
PROMPT# clear snmp notify target 3
success: change accepted.
```

See Also

- 1 **set snmp notify target** on page 137
- 1 **show snmp notify target** on page 174

clear snmp usm

Clears an SNMPv3 user.

Syntax **clear snmp usm** *usm-username*

usm-username Name of the SNMPv3 user you want to clear.

Defaults None.

Access Enabled.

Examples The following command clears SNMPv3 user *snmpmgr1*:

```
PROMPT# clear snmp usm snmpmgr1
success: change accepted.
```

See Also

- 1 **set snmp usm** on page 146
- 1 **show snmp usm** on page 175

clear summertime

Clears the summertime setting from a UNIVERGE WL Controller.

Syntax **clear summertime**

Defaults None.

Access Enabled.

Examples To clear the summertime setting from a UNIVERGE WL Controller, type the following command:

```
PROMPT# clear summertime
success: change accepted.
```

clear system ip-address

Chapter 8

See Also

- 1 **clear timezone** on page 107
- 1 **set summertime** on page 151
- 1 **set timedate** on page 154
- 1 **set timezone** on page 155
- 1 **show summertime** on page 175
- 1 **show timedate** on page 176
- 1 **show timezone** on page 177

clear system ip-address

Clears the system IP address.



Caution! Clearing the system IP address disrupts the system tasks that use the address.

Syntax **clear system ip-address**

Defaults None.

Access Enabled.

Usage Clearing the system IP address can interfere with system tasks that use the system IP address, including the following:

- 1 Mobility Domain operations
- 1 Topology reporting for dual-homed AP
- 1 Default source IP address used in unsolicited communications such as AAA accounting reports and SNMP traps

Examples To clear the system IP address, type the following command:

```
PROMPT# clear system ip-address
success: change accepted.
```

See Also

- 1 **set system ip-address** on page 153
- 1 **show system** on page 40

clear timezone

Clears the time offset for the UNIVERGE WL Controller real-time clock from Coordinated Universal Time (UTC). UTC is also known as Greenwich Mean Time (GMT).

Syntax clear timezone

Defaults None.

Access Enabled.

Examples To return the UNIVERGE WL Controller real-time clock to UTC, type the following command:

```
PROMPT# clear timezone
success: change accepted.
```

See Also

- 1 **clear summertime** on page 105
- 1 **set summertime** on page 151
- 1 **set timedate** on page 154
- 1 **set timezone** on page 155
- 1 **show summertime** on page 175
- 1 **show timedate** on page 176
- 1 **show timezone** on page 177

ping

Tests IP connectivity between a UNIVERGE WL Controller and another device. UNIVERGE WL Control System sends an Internet Control Message Protocol (ICMP) echo packet to the specified device and listens for a reply packet.

Syntax **ping** *host* [**count** *num-packets*] [**dnf**] [**flood**] [**interval** *time*] [**size** *size*]

<i>host</i>	IP address, MAC address, hostname, alias, or user to ping.
count <i>num-packets</i>	Number of ping packets to send. You can specify from 0 through 2,147,483,647. If you enter 0, UNIVERGE WL Control System pings continuously until you interrupt the command.
dnf	Enables the Do Not Fragment bit in the ping packet to prevent fragmenting the packet.
flood	Sends new ping packets as quickly as replies are received, or 100 times per second, whichever is greater.

Note: Use the **flood** option sparingly. This option creates a lot of traffic and can affect other traffic on the network.

interval <i>time</i>	Time interval between ping packets, in milliseconds. You can specify from 100 through 10,000.
size <i>size</i>	Packet size, in bytes. You can specify from 56 through 65,507.

Note: Because the UNIVERGE WL Controller adds header information, the ICMP packet size is 8 bytes larger than the size you specify.

Defaults

- 1 **count**—5.
- 1 **dnf**—Disabled.
- 1 **interval**—100 (one tenth of a second)
- 1 **size**—56.

Access Enabled.

Usage To stop a **ping** command that is in progress, press Ctrl+C.

A UNIVERGE WL Controller cannot ping itself. UNIVERGE WL Control System does not support this.
A UNIVERGE WL Controller does not support **interval** option.

Examples The following command pings a device that has IP address 10.1.1.1:

```
PROMPT# ping 10.1.1.1
PING 10.1.1.1 (10.1.1.1) from 10.9.4.34 : 56(84) bytes of data.
64 bytes from 10.1.1.1: icmp_seq=1 ttl=255 time=0.769 ms
64 bytes from 10.1.1.1: icmp_seq=2 ttl=255 time=0.628 ms
64 bytes from 10.1.1.1: icmp_seq=3 ttl=255 time=0.676 ms
64 bytes from 10.1.1.1: icmp_seq=4 ttl=255 time=0.619 ms
64 bytes from 10.1.1.1: icmp_seq=5 ttl=255 time=0.608 ms
--- 10.1.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0 errors, 0% packet loss
```

See Also **traceroute** on page 179

set arp

Adds an ARP entry to the ARP table.

Syntax **set arp** {**permanent** | **static** | **dynamic**} *ip-addr mac-addr*

permanent	Adds a permanent entry. A permanent entry does not age out and remains in the database even after a reboot, reset, or power cycle.
static	Adds a static entry. A static entry does not age out, but the entry does not remain in the database after a reboot, reset, or power cycle.
dynamic	Adds a dynamic entry. A dynamic entry is automatically removed if the entry ages out, or after a reboot, reset, or power cycle.
<i>ip-addr</i>	IP address of the entry, in dotted decimal notation.
<i>mac-addr</i>	MAC address to map to the IP address. Use colons to separate the octets (for example, 00:11:22:aa:bb:cc).

Defaults None.

Access Enabled.

set arp agingtime

Chapter 8

Examples The following command adds a static ARP entry that maps IP address 10.10.10.1 to MAC address 00:bb:cc:dd:ee:ff:

```
PROMPT# set arp static 10.10.10.1 00:bb:cc:dd:ee:ff
success: added arp 10.10.10.1 at 00:bb:cc:dd:ee:ff on VLAN 1
```

See Also

- 1 **set arp agingtime** on page 110
- 1 **show arp** on page 156

set arp agingtime

Changes the aging timeout for dynamic ARP entries.

Syntax **set arp agingtime** *seconds*

seconds Number of seconds an entry can remain unused before UNIVERGE WL Control System removes the entry. You can specify from 0 through 1,000,000. To disable aging, specify 0.

Defaults The default aging timeout is 1200 seconds.

Access Enabled.

Usage Aging applies only to dynamic entries.

To reset the ARP aging timeout to its default value, use the **set arp agingtime 1200** command.

Examples The following command changes the ARP aging timeout to 1800 seconds:

```
PROMPT# set arp agingtime 1800
success: set arp aging time to 1800 seconds
```

The following command disables ARP aging:

```
PROMPT# set arp agingtime 0
success: set arp aging time to 0 seconds
```

See Also

- 1 **set arp** on page 109
- 1 **show arp** on page 156

set interface

Configures an IP interface on a VLAN.

Syntax **set interface** *vlan-id* **ip** {*ip-addr mask* | *ip-addr/mask-length*}

<i>vlan-id</i>	VLAN name or number.
<i>ip-addr mask</i>	IP address and subnet mask in dotted decimal notation (for example, 10.10.10.10 255.255.255.0).
<i>ip-addr/mask-length</i>	IP address and subnet mask length in CIDR format (for example, 10.10.10.10/24).

Defaults None.

Access Enabled.

Usage You can assign one IP interface to each VLAN.

If an interface is already configured on the specified VLAN, this command replaces the interface. If you replace an interface that is in use as the system IP address, replacing the interface can interfere with system tasks that use the system IP address, including the following:

- 1 Mobility domain operations
- 1 Topology reporting for dual-homed AP
- 1 Default source IP address used in unsolicited communications such as AAA accounting reports and SNMP traps

Examples The following command configures IP interface 10.10.10.10/24 on VLAN *default*:

```
PROMPT# set interface default ip 10.10.10.10/24
success: set ip address 10.10.10.10 netmask 255.255.255.0 on vlan default
```

set interface dhcp-client

Chapter 8

The following command configures IP interface 10.10.20.10 255.255.255.0 on VLAN *mauve*:

```
PROMPT# set interface mauve ip 10.10.20.10 255.255.255.0
success: set ip address 10.10.20.10 netmask 255.255.255.0 on vlan mauve
```

See Also

- 1 **clear interface** on page 97
- 1 **set interface status** on page 115
- 1 **show interface** on page 161

set interface dhcp-client

Configures the DHCP client on a VLAN and allows the VLAN to obtain its IP interface from a DHCP server.

Syntax **set interface** *vlan-id* **ip dhcp-client** { **enable** | **disable** }

<i>vlan-id</i>	VLAN name or number.
enable	Enables the DHCP client on the VLAN.
disable	Disables the DHCP client on the VLAN.

Defaults The DHCP client is enabled by default

Access Enabled.

Usage You can enable the DHCP client on one VLAN only. You can configure the DHCP client on more than one VLAN, but the client can be active on only one VLAN.

UNIVERGE WL Control System also has a configurable DHCP server. (See **set interface dhcp-server** on page 113.) You can configure a DHCP client and DHCP server on the same VLAN, but only the client or the server can be enabled. The DHCP client and DHCP server cannot both be enabled on the same VLAN at the same time.

Examples The following command enables the DHCP client on VLAN *corpvlan*:

```
PROMPT# set interface corpvlan ip dhcp-client enable
success: change accepted.
```

See Also

- 1 **clear interface** on page 97
- 1 **show dhcp-client** on page 157
- 1 **show interface** on page 161

set interface dhcp-server

Configures the UNIVERGE WL Control System DHCP server.



Note. Use of the UNIVERGE WL Control System DHCP server to allocate client addresses is intended for temporary, demonstration deployments and not for production networks. It is recommended that you do not use the UNIVERGE WL Control System DHCP server to allocate client addresses in a production network.

Syntax **set interface** *vlan-id* **ip dhcp-server** [**enable** | **disable**] [**start** *ip-addr1* **stop** *ip-addr2*] [**dns-domain** *domain-name*] [**primary-dns** *ip-addr* [**secondary-dns** *ip-addr*]] [**default-router** *ip-addr*]

<i>vlan-id</i>	VLAN name or number.
enable	Enables the DHCP server.
disable	Disables the DHCP server.
start <i>ip-addr1</i>	Specifies the beginning address of the address range (also called the address <i>pool</i>).
stop <i>ip-addr2</i>	Specifies the ending address of the address range.
dns-domain <i>domain-name</i>	Name of the DHCP client's default DNS domain.

set interface dhcp-server

Chapter 8

- primary-dns** *ip-addr* IP addresses of the DHCP client's DNS servers.
[**secondary-dns** *ip-addr*]
default-router *ip-addr* IP address of the DHCP client's default router.

Defaults The DHCP server is enabled by default.

Access Enabled.

Usage By default, all addresses except the host address of the VLAN, the network broadcast address, and the subnet broadcast address are included in the range. If you specify the range, the start address must be lower than the stop address, and all addresses must be in the same subnet. The IP interface of the VLAN must be within the same subnet but is not required to be within the range.

Specification of the DNS domain name, DNS servers, and default router are optional. If you omit one or more of these options, the UNIVERGE WL Control System DHCP server uses oath values configured elsewhere on the switch:

- 1 DNS domain name—If this option is not set with the **set interface dhcp-server** command **dns-domain** option, the UNIVERGE WL Control System DHCP server uses the value set by the **set ip dns domain** command.
- 1 DNS servers—If these options are not set with the **set interface dhcp-server** command **primary-dns** and **secondary-dns** options, the UNIVERGE WL Control System DHCP server uses the values set by the **set ip dns server** command.
- 1 Default router—If this option is not set with the **set interface dhcp-server** command **default-router** option, the UNIVERGE WL Control System DHCP server can use the value set by the **set ip route** command. A default route configured by **set ip route** can be used if the route is in the DHCP client subnet. Otherwise, the UNIVERGE WL Control System DHCP server does not specify a router address.

Examples The following command enables the DHCP server on VLAN *red-vlan* to serve addresses from the 192.168.1.5 to 192.168.1.25 range:

```
PROMPT# set interface red-vlan ip dhcp-server enable start 192.168.1.5 stop  
192.168.1.25  
success: change accepted.
```

See Also

- 1 **set ip dns domain** on page 117

- 1 **set ip dns server** on page 118
- 1 **show dhcp-server** on page 159

set interface status

Administratively disables or reenables an IP interface.

Syntax `set interface vlan-id status {up | down}`

<i>vlan-id</i>	VLAN name or number.
up	Enables the interface.
down	Disables the interface.

Defaults IP interfaces are enabled by default.

Access Enabled.

Examples The following command disables the IP interface on VLAN *mauve*:

```
PROMPT# set interface mauve status down
success: set interface mauve to down
```

See Also

- 1 **clear interface** on page 97
- 1 **set interface** on page 111
- 1 **show interface** on page 161

set ip alias

Configures an alias, which maps a name to an IP address. You can use aliases as shortcuts in CLI commands.

set ip dns

Chapter 8

Syntax `set ip alias name ip-addr`

name String of up to 32 alphanumeric characters, with no spaces.

ip-addr IP address in dotted decimal notation.

Defaults None.

Access Enabled.

Examples The following command configures the alias *HR1* for IP address 192.168.1.2:

```
PROMPT# set ip alias HR1 192.168.1.2
success: change accepted.
```

See Also

1 **clear ip alias** on page 98

1 **show ip alias** on page 163

set ip dns

Enables or disables DNS on a UNIVERGE WL Controller.

Syntax `set ip dns {enable | disable}`

enable Enables DNS.

disable Disables DNS.

Defaults DNS is disabled by default.

Access Enabled.

Examples The following command enables DNS on a UNIVERGE WL Controller:

```
PROMPT# set ip dns enable
Start DNS Client
```

See Also

- 1 **clear ip dns domain** on page 99
- 1 **clear ip dns server** on page 99
- 1 **set ip dns domain** on page 117
- 1 **set ip dns server** on page 118
- 1 **show ip dns** on page 164

set ip dns domain

Configures a default domain name for DNS queries. The UNIVERGE WL Controller appends the default domain name to domain names or hostnames you enter in commands.

Syntax **set ip dns domain** *name*

name Domain name of between 1 and 64 alphanumeric characters with no spaces (for example, example.org).

Defaults None.

Access Enabled.

Usage To override the default domain name when entering a hostname in a CLI command, enter a period at the end of the hostname. For example, if the default domain name is *example.com*, enter **chris.** if the fully qualified hostname is *chris* and not *chris.example.com*.

Aliases take precedence over DNS. When you enter a hostname, UNIVERGE WL Control System checks for an alias with that name first, before using DNS to resolve the name.

Examples The following command configures the default domain name *example.com*:

```
PROMPT# set ip dns domain example.com
Domain name changed
```

See Also

- 1 **clear ip dns domain** on page 99
- 1 **clear ip dns server** on page 99
- 1 **set ip dns** on page 116
- 1 **set ip dns server** on page 118
- 1 **show ip dns** on page 164

set ip dns server

Specifies a DNS server to use for resolving hostnames you enter in CLI commands.

Syntax **set ip dns server** *ip-addr* {**primary** | **secondary**}

<i>ip-addr</i>	IP address of a DNS server, in dotted decimal or CIDR notation.
primary	Defines the server as the primary server that UNIVERGE WL Control System always consults first for resolving DNS queries.
secondary	Defines the server as a secondary server. UNIVERGE WL Control System consults a secondary server only if the primary server does not reply.

Defaults None.

Access Enabled.

Usage You can configure a UNIVERGE WL Controller to use one primary DNS server and up to five secondary DNS servers.

Examples The following commands configure a UNIVERGE WL Controller to use a primary DNS server and two secondary DNS servers:

```
PROMPT# set ip dns server 10.10.10.50/24 primary
success: change accepted.
PROMPT# set ip dns server 10.10.20.69/24 secondary
```

success: change accepted.

```
PROMPT# set ip dns server 10.10.30.69/24 secondary
```

success: change accepted.

See Also

- 1 **clear ip dns domain** on page 99
- 1 **clear ip dns server** on page 99
- 1 **set ip dns** on page 116
- 1 **set ip dns domain** on page 117
- 1 **show ip dns** on page 164

set ip https server

Enables the HTTPS server on a UNIVERGE WL Controller. The HTTPS server is required for WebView access to the UNIVERGE WL Controller.



Caution! If you disable the HTTPS server, WebView access to the UNIVERGE WL Controller is disabled.

Syntax `set ip https server {enable | disable}`

enable Enables the HTTPS server.

disable Disables the HTTPS server.

Defaults The HTTPS server is enabled by default.

Access Enabled.

Examples The following command disables the HTTPS server on a UNIVERGE WL Controller:

```
PROMPT# set ip https server disable
```

success: change accepted.

See Also

- 1 **clear ip telnet** on page 101

- 1 **set ip telnet** on page 125
- 1 **set ip telnet server** on page 126
- 1 **show ip https** on page 165
- 1 **show ip telnet** on page 169

set ip route

Adds a static route to the IP route table.

Syntax **set ip route** {**default** | *ip-addr mask* | *ip-addr/mask-length*}
default-router metric

default

Default route. A UNIVERGE WL Controller uses the default route if an explicit route is not available for the destination.

Note: **default** is an alias for IP address 0.0.0.0/0.

ip-addr mask

IP address and subnet mask for the route destination, in dotted decimal notation (for example, 10.10.10.10 255.255.255.0).

ip-addr/mask-length

IP address and subnet mask length in CIDR format (for example, 10.10.10.10/24).

default-router

IP address, DNS hostname, or alias of the next-hop router.

metric

Cost for using the route. You can specify a value from 0 through 2,147,483,647. Lower-cost routes are preferred over higher-cost routes.

Defaults None.

Access Enabled.

Usage UNIVERGE WL Control System can use a static route only if a direct route in the route table resolves the static route. UNIVERGE WL Control System adds routes with next-hop types Local and Direct when you add an IP interface to a VLAN, if the VLAN is up. If one of these added routes can resolve the static route, UNIVERGE WL Control System can use the static route.

Before you add a static route, use the **show interface** command to verify that the UNIVERGE WL Controller has an IP interface in the same subnet as the next-hop router. If not, the VLAN:Interface field of the **show ip route** command output shows that the route is down.

You can configure a maximum of 4 routes per destination. This includes default routes, which have destination 0.0.0.0/0. Each route to a given destination must have a unique router address. When the route table contains multiple default or explicit routes to the same destination, UNIVERGE WL Control System uses the route with the lowest cost. If two or more routes to the same destination have the lowest cost, UNIVERGE WL Control System selects the first route in the route table.

When you add multiple routes to the same destination, UNIVERGE WL Control System groups the routes and orders them from lowest cost at the top of the group to highest cost at the bottom of the group. If you add a new route that has the same destination and cost as a route already in the table, UNIVERGE WL Control System places the new route at the top of the group of routes with the same cost.

Examples The following command adds a default route that uses default router 10.5.4.1 and gives the route a cost of 1:

```
PROMPT# set ip route default 10.5.4.1 1
success: change accepted.
```

The following commands add two default routes, and configure UNIVERGE WL Control System to always use the route through 10.2.4.69 when the UNIVERGE WL Controller interface to that default router is up:

```
PROMPT# set ip route default 10.2.4.69 1
success: change accepted.

PROMPT# set ip route default 10.2.4.17 2
success: change accepted.
```

set ip snmp server

Chapter 8

The following command adds an explicit route from a UNIVERGE WL Controller to any host on the 192.168.4.x subnet through the local router 10.5.4.2, and gives the route a cost of 1:

```
PROMPT# set ip route 192.168.4.0 255.255.255.0 10.5.4.2 1
success: change accepted.
```

The following command adds another explicit route, using CIDR notation to specify the subnet mask:

```
PROMPT# set ip route 192.168.5.0/24 10.5.5.2 1
success: change accepted.
```

- 1 **clear ip route** on page 100
- 1 **show interface** on page 161
- 1 **show ip route** on page 167

set ip snmp server

Enables or disables the SNMP service on the UNIVERGE WL Controller.

Syntax **set ip snmp server** {**enable** | **disable**}

enable Enables the SNMP service.

disable Disables the SNMP service.

Defaults The SNMP service is disabled by default.

Access Enabled.

Examples The following command enables the SNMP server on a UNIVERGE WL Controller:

```
PROMPT# set ip snmp server enable
success: change accepted.
```

See Also

- 1 **clear snmp usm** on page 105
- 1 **set port trap** on page 61

- 1 **set snmp community** on page 130
- 1 **set snmp usm** on page 146
- 1 **set snmp notify profile** on page 132
- 1 **show snmp community** on page 173

set ip ssh

Changes the TCP port number on which a UNIVERGE WL Controller listens for Secure Shell (SSH) management traffic.



Caution! If you change the SSH port number from an SSH session, UNIVERGE WL Control System immediately ends the session. To open a new management session, you must configure the SSH client to use the new TCP port number.

Syntax **set ip ssh port** *port-num*

port-num TCP port number.

Defaults The default SSH port number is 22.

Access Enabled.

Examples The following command changes the SSH port number on a UNIVERGE WL Controller to 6000:

```
PROMPT# set ip ssh port 6000
success: change accepted.
```

See Also

- 1 **set ip ssh server** on page 124
- 1 **set ip ssh server** on page 124
- 1 **set ip ssh server** on page 124

set ip ssh server

Disables or reenables the SSH server on a UNIVERGE WL Controller.



Caution! If you disable the SSH server, SSH access to the UNIVERGE WL Controller is also disabled.

Syntax `set ip ssh server {enable | disable}`

enable Enables the SSH server.

disable Disables the SSH server.

Defaults The SSH server is enabled by default.

Access Enabled.

Usage SSH requires an SSH authentication key. You can generate one or allow UNIVERGE WL Control System to generate one. The first time an SSH client attempts to access the SSH server on a UNIVERGE WL Controller, the UNIVERGE WL Controller automatically generates a 1024-byte SSH key. If you want to use a 2048-byte key instead, use the **crypto generate key ssh 2048** command to generate one.

The maximum number of SSH sessions supported on a UNIVERGE WL Controller is eight. If Telnet is also enabled, the UNIVERGE WL Controller can have up to eight Telnet or SSH sessions, in any combination.

See Also

- 1 **crypto generate key** on page 485
- 1 **set ip ssh** on page 123
- 1 **set ip ssh server** on page 124
- 1 **set ip ssh server** on page 124

set ip telnet

Changes the TCP port number on which a UNIVERGE WL Controller listens for Telnet management traffic.



Caution! If you change the Telnet port number from a Telnet session, UNIVERGE WL Control System immediately ends the session. To open a new management session, you must Telnet to the UNIVERGE WL Controller with the new Telnet port number.

Syntax `set ip telnet port-num`

port-num TCP port number.

Defaults The default Telnet port number is 23.

Access Enabled.

Examples The following command changes the Telnet port number on a UNIVERGE WL Controller to 5000:

```
PROMPT# set ip telnet 5000
success: change accepted.
```

See Also

- 1 **clear ip telnet** on page 101
- 1 **set ip https server** on page 119
- 1 **set ip telnet server** on page 126
- 1 **show ip https** on page 165
- 1 **show ip telnet** on page 169

set ip telnet server

Enables the Telnet server on a UNIVERGE WL Controller.



Caution! If you disable the Telnet server, Telnet access to the UNIVERGE WL Controller is also disabled.

Syntax `set ip telnet server {enable | disable}`

enable Enables the Telnet server.

disable Disables the Telnet server.

Defaults The Telnet server is enabled by default.

Access Enabled.

Usage The maximum number of Telnet sessions supported on a UNIVERGE WL Controller is eight. If SSH is also enabled, the UNIVERGE WL Controller can have up to eight Telnet or SSH sessions, in any combination.

Examples The following command disables the Telnet server on a UNIVERGE WL Controller:

```
PROMPT# set ip telnet server disable
success: change accepted.
```

See Also

- 1 **clear ip telnet** on page 101
- 1 **set ip https server** on page 119
- 1 **set ip telnet** on page 125
- 1 **show ip https** on page 165
- 1 **show ip telnet** on page 169

set ntp

Enables or disables the NTP client on a UNIVERGE WL Controller.

Syntax **set ntp** {**enable** | **disable**}

enable Enables the NTP client.

disable Disables the NTP client.

Defaults The NTP client is disabled by default.

Access Enabled.

Usage If NTP is configured on a system whose current time differs from the NTP server time by more than 10 minutes, convergence of the UNIVERGE WL Controller time can take many NTP update intervals. It is recommended that you set the time manually to the NTP server time before enabling NTP to avoid a significant delay in convergence.

Examples The following command enables the NTP client:

```
PROMPT# set ntp enable
success: NTP Client enabled
```

See Also

- 1 **clear ntp server** on page 102
- 1 **clear ntp update-interval** on page 102
- 1 **set ntp server** on page 128
- 1 **set ntp update-interval** on page 129
- 1 **show ntp** on page 170

set ntp server

Configures a UNIVERGE WL Controller to use an NTP server.

Syntax **set ntp server** *ip-addr*

ip-addr IP address of the NTP server, in dotted decimal notation.

Defaults None.

Access Enabled.

Usage You can configure up to three NTP servers. UNIVERGE WL Control System queries all the servers and selects the best response based on the method described in RFC 1305, *Network Time Protocol (Version 3) Specification, Implementation and Analysis*.

To use NTP, you also must enable the NTP client with the **set ntp** command.

Examples The following command configures a UNIVERGE WL Controller to use NTP server 192.168.1.5:

```
PROMPT# set ntp server 192.168.1.5
```

See Also

- 1 **clear ntp server** on page 102
- 1 **clear ntp update-interval** on page 102
- 1 **set ntp** on page 127
- 1 **set ntp update-interval** on page 129
- 1 **show ntp** on page 170

set ntp update-interval

Changes how often a UNIVERGE WL Control System sends queries to the NTP servers for updates.

Syntax `set ntp update-interval seconds`

seconds Number of seconds between queries. You can specify from 16 through 1024 seconds.

Defaults The default NTP update interval is 64 seconds.

Access Enabled.

Examples The following command changes the NTP update interval to 128 seconds:

```
PROMPT# set ntp update-interval 128
success: change accepted.
```

See Also

- 1 **clear ntp server** on page 102
- 1 **clear ntp update-interval** on page 102
- 1 **set ntp** on page 127
- 1 **set ntp server** on page 128
- 1 **show ntp** on page 170

set snmp community

Configures a community string for SNMPv1 or SNMPv2c.



Note. For SNMPv3, use the **set snmp usm** command to configure an SNMPv3 user. SNMPv3 does not use community strings.

Syntax **set snmp community name** *comm-string*
access { **read-only** | **read-notify** | **notify-only** | **read-write** | **notify-read-write** }

comm-string Name of the SNMP community. Specify between 1 and 32 alphanumeric characters, with no spaces.

read-only Allows an SNMP management application using the string to get (read) object values on the UNIVERGE WL Controller but not to set (write) them.

read-notify Allows an SNMP management application using the string to get object values on the UNIVERGE WL Controller but not to set them. The UNIVERGE WL Controller can use the string to send notifications.

notify-only Allows the UNIVERGE WL Controller to use the string to send notifications.

read-write Allows an SNMP management application using the string to get and set object values on the UNIVERGE WL Controller.

notify-read-write Allows an SNMP management application using the string to get and set object values on the UNIVERGE WL Controller. The UNIVERGE WL Controller also can use the string to send notifications.

Defaults None.

Access Enabled.

Usage SNMP community strings are passed as clear text in SNMPv1 and SNMPv2c. UNIVERGE WL Control System recommends that you use strings that cannot easily be guessed by unauthorized users. For example, do not use the well-known strings *public* and *private*.

If you are using SNMPv3, you can configure SNMPv3 users to use authentication and to encrypt SNMP data.

Examples The following command configures the read-write community *good_community*:

```
PROMPT# set snmp community read-write good_community
success: change accepted.
```

The following command configures community string *switchmgr1* with access level **notify-read-write**:

```
PROMPT# set snmp community name switchmgr1 notify-read-write
success: change accepted.
```

See Also

- 1 **clear snmp community** on page 103
- 1 **set ip snmp server** on page 122
- 1 **set snmp notify target** on page 137
- 1 **set snmp notify profile** on page 132
- 1 **set snmp protocol** on page 143
- 1 **set snmp security** on page 144
- 1 **set snmp usm** on page 146
- 1 **show snmp community** on page 173

set snmp notify profile

Configures an SNMP notification profile. A *notification profile* is a named list of all the notification types that can be generated by a UNIVERGE WL Controller, and for each notification type, the action to take (drop or send) when an event occurs.

You can configure up to ten notification profiles.

Syntax **set snmp notify profile** { **default** | *profile-name* }
{ **drop** | **send** } { *notification-type* | **all** }

default |
profile-name

Name of the notification profile you are creating or modifying. The *profile-name* can be up to 32 alphanumeric characters long, with no spaces.

To modify the default notification profile, specify **default**.

drop | **send**

Specifies the action that the SNMP engine takes with regard to the notifications you specify with *notification-type* or **all**.

notification-type

Name of the notification type:

- **APBootTraps**—Generated when a UNIVERGE WL Access Point boots.
- **ApNonOperStatusTraps**—Generated to indicate a UNIVERGE WL Access Point radio is nonoperational.
- **ApOperRadioStatusTraps**—Generated when the status of a UNIVERGE WL Access Point radio changes.
- **APTimeoutTraps**—Generated when an AP fails to respond to the UNIVERGE WL Controller.
- **AuthenTraps**—Generated when the UNIVERGE WL Controllers SNMP engine receives a bad community string.
- **AutoTuneRadioChannelChangeTraps**—Generated when the RF Auto-Tuning feature changes the channel on a radio.
- **AutoTuneRadioPowerChangeTraps**—Generated when the RF Auto-Tuning feature changes the power setting on a radio.
- **ClientAssociationFailureTraps**—Generated when a client's attempt to associate with a radio fails.
- **ClientAuthorizationSuccessTraps**—Generated when a client is successfully authorized.
- **ClientAuthenticationFailureTraps**—Generated when authentication fails for a client.
- **ClientAuthorizationFailureTraps**—Generated when authorization fails for a client.
- **ClientClearedTraps**—Generated when a client's session is cleared.
- **ClientDeAssociationTraps**—Generated when a client is dissociated from a radio.
- **ClientDot1xFailureTraps**—Generated when a client experiences an 802.1X failure.
- **ClientRoamingTraps**—Generated when a client roams.
- **CounterMeasureStartTraps**—Generated when UNIVERGE WL Control System begins countermeasures against a rogue access point.

notification-type
(cont.)

- **CounterMeasureStopTraps**—Generated when UNIVERGE WL Control System stops countermeasures against a rogue access point.
- **DAPConnectWarningTraps**—Generated when a UNIVERGE WL Access Points whose fingerprint has not been configured in UNIVERGE WL Control System establishes a management session with the UNIVERGE WL Controller.
- **DeviceFailTraps**—Generated when an event with an Alert severity occurs.
- **DeviceOkayTraps**—Generated when a device returns to its normal state.
- **LinkDownTraps**—Generated when the link is lost on a port.
- **LinkUpTraps**—Generated when the link is detected on a port.
- **MichaelMICFailureTraps**—Generated when two Michael message integrity code (MIC) failures occur within 60 seconds, triggering Wi-Fi Protected Access (WPA) countermeasures.
- **MobilityDomainJoinTraps**—Generated when the UNIVERGE WL Controller is initially able to contact a mobility domain seed member, or can contact the seed member after a timeout.
- **MobilityDomainTimeoutTraps**—Generated when a timeout occurs after a UNIVERGE WL Controller has unsuccessfully tried to communicate with a seed member.
- **PoEFailTraps**—Generated when a serious PoE problem, such as a short circuit, occurs.
- **RFDetectAdhocUserTraps**—Generated when UNIVERGE WL Control System detects an ad-hoc user.
- **RFDetectRogueAPTraps**—Generated when UNIVERGE WL Control System detects a rogue access point.
- **RFDetectRogueDisappearTraps**—Generated when a rogue access point is no longer being detected.
- **RFDetectClientViaRogueWiredAPTraps**—Generated when UNIVERGE WL Control System detects, on the wired part of the network, the MAC address of a wireless client associated with a third-party AP.

notification-type
(cont.)

- **RFDetectDoSPortTraps**—Generated when UNIVERGE WL Control System detects an associate request flood, reassociate request flood, or disassociate request flood.
- **RFDetectDoSTraps**—Generated when UNIVERGE WL Control System detects a DoS attack other than an associate request flood, reassociate request flood, or disassociate request flood.
- **RFDetectInterferingRogueAPTraps**—Generated when an interfering device is detected.
- **RFDetectInterferingRogueDisappearTraps**—Generated when an interfering device is no longer detected.
- **RFDetectSpoofedMacAPTraps**—Generated when UNIVERGE WL Control System detects a wireless packet with the source MAC address of a UNIVERGE WL Access Points, but without the spoofed UNIVERGE WL Access Points signature (fingerprint).
- **RFDetectSpoofedSsidAPTraps**—Generated when UNIVERGE WL Control System detects beacon frames for a valid SSID, but sent by a rogue AP.
- **RFDetectUnauthorizedAPTraps**—Generated when UNIVERGE WL Control System detects the MAC address of an AP that is on the attack list.
- **RFDetectUnauthorizedOuiTraps**—Generated when a wireless device that is not on the list of permitted vendors is detected.
- **RFDetectUnauthorizedSsidTraps**—Generated when an SSID that is not on the permitted SSID list is detected.

all Sends or drops all notifications.

Defaults A default notification profile (named *default*) is already configured on the UNIVERGE WL Control System. All notifications in the default profile are dropped by default.

Access Enabled.

set snmp notify profile

Chapter 8

Examples The following command changes the action in the default notification profile from **drop** to **send** for all notification types:

```
PROMPT# set snmp notify profile default send all
success: change accepted.
```

The following commands create notification profile *snmpprof_rfdetect*, and change the action to **send** for all RF detection notification types:

```
PROMPT# set snmp notify profile snmpprof_rfdetect send RFDetectAdhocUserTraps
success: change accepted.
```

```
PROMPT# set snmp notify profile snmpprof_rfdetect send
RFDetectClientViaRogueWiredAPTraps
success: change accepted.
```

```
PROMPT# set snmp notify profile snmpprof_rfdetect send RFDetectDoSTraps
success: change accepted.
```

```
PROMPT# set snmp notify profile snmpprof_rfdetect send RFDetectAdhocUserTraps
success: change accepted.
```

```
PROMPT# set snmp notify profile snmpprof_rfdetect send
RFDetectInterferingRogueAPTraps
success: change accepted.
```

```
PROMPT# set snmp notify profile snmpprof_rfdetect send
RFDetectInterferingRogueDisappearTraps
success: change accepted.
```

```
PROMPT# set snmp notify profile snmpprof_rfdetect send RFDetectRogueAPTraps
success: change accepted.
```

```
PROMPT# set snmp notify profile snmpprof_rfdetect send
RFDetectRogueDisappearTraps
success: change accepted.
```

```
PROMPT# set snmp notify profile snmpprof_rfdetect send
RFDetectSpoofedMacAPTraps
success: change accepted.
```

```
PROMPT# set snmp notify profile snmpprof_rfdetect send
RFDetectSpoofedSsidAPTraps
success: change accepted.
```

```
PROMPT# set snmp notify profile snmpprof_rfdetect send
RFDetectUnauthorizedAPTraps
success: change accepted.
```

```
PROMPT# set snmp notify profile snmpprof_rfdetect send
RFDetectUnauthorizedOuiTraps
success: change accepted.
```

```
PROMPT# set snmp notify profile snmpprof_rfdetect send
RFDetectUnauthorizedSsidTraps
success: change accepted.
```

See Also

- 1 **clear snmp notify profile** on page 103
- 1 **set ip snmp server** on page 122
- 1 **set snmp community** on page 130
- 1 **set snmp notify target** on page 137
- 1 **set snmp protocol** on page 143
- 1 **set snmp security** on page 144
- 1 **set snmp usm** on page 146
- 1 **show snmp notify profile** on page 173

set snmp notify target

Configures a notification target for notifications from SNMP.

A notification target is a remote device that the UNIVERGE WL Control System sends SNMP notifications to. You can configure the UNIVERGE WL Control System SNMP engine to send confirmed notifications (informs) or unconfirmed notifications (traps). Some of the command options differ depending on the SNMP version and the type of notification you specify. You can configure up to 10 notification targets.

SNMPv3 with Informs

To configure a notification target for informs from SNMPv3, use the following command:

Syntax **set snmp notify target** *target-num ip-addr[:udp-port-number]*
usm inform user *username*
snmp-engine-id {**ip** | **hex** *hex-string*}
[profile *profile-name*]
[security {**unsecured** | **authenticated** | **encrypted**}]
[retries *num*]
[timeout *num*]

set snmp notify target

Chapter 8

<i>target-num</i>	ID for the target. This ID is local to the UNIVERGE WL Controller and does not need to correspond to a value on the target itself. You can specify a number from 1 to 10.
<i>ip-addr[:udp-port-number]</i>	IP address of the server. You also can specify the UDP port number to send notifications to.
<i>username</i>	USM username. This option is applicable only when the SNMP version is usm . If the user will send informs rather than traps, you also must specify the snmp-engine-id of the target.
snmp-engine-id { ip hex <i>hex-string</i> }	SNMP engine ID of the target. Specify ip if the target SNMP engine ID is based on its IP address. If the target's SNMP engine ID is a hexadecimal value, use hex <i>hex-string</i> to specify the value.
profile <i>profile-name</i>	Notification profile that this SNMP user will use to specify the notification types to send or drop.
security { unsecured authenticated encrypted }	Specifies the security level, and is applicable only when the SNMP version is usm : <ul style="list-style-type: none">• unsecured—Message exchanges are not authenticated, nor are they encrypted. This is the default.• authenticated—Message exchanges are authenticated, but are not encrypted.• encrypted—Message exchanges are authenticated and encrypted.

retries <i>num</i>	Specifies the number of times the UNIVERGE WL Control System SNMP engine will resend a notification that has not been acknowledged by the target. You can specify from 0 to 3 retries.
timeout <i>num</i>	Specifies the number of seconds UNIVERGE WL Control System waits for acknowledgement of a notification. You can specify from 1 to 5 seconds.

SNMPv3 with Traps

To configure a notification target for traps from SNMPv3, use the following command:

Syntax **set snmp notify target** *target-num ip-addr[:udp-port-number]*
usm trap user *username*
[profile *profile-name***]**
[security { unsecured | authenticated | encrypted }]

<i>target-num</i>	ID for the target. This ID is local to the UNIVERGE WL Controller and does not need to correspond to a value on the target itself. You can specify a number from 1 to 10.
<i>ip-addr[:udp-port-number]</i>	IP address of the server. You also can specify the UDP port number to send notifications to.
<i>username</i>	USM username. This option is applicable only when the SNMP version is usm .

set snmp notify target

Chapter 8

profile <i>profile-name</i>	Notification profile this SNMP user will use to specify the notification types to send or drop.
security { unsecured authenticated encrypted }	Specifies the security level, and is applicable only when the SNMP version is usm : <ul style="list-style-type: none">• unsecured—Message exchanges are not authenticated, nor are they encrypted. This is the default.• authenticated—Message exchanges are authenticated, but are not encrypted.• encrypted—Message exchanges are authenticated and encrypted.

SNMPv2c with Informs

To configure a notification target for informs from SNMPv2c, use the following command:

Syntax **set snmp notify target** *target-num ip-addr[:udp-port-number]*
v2c *community-string* **inform**
[**profile** *profile-name*]
[**retries** *num*]
[**timeout** *num*]

<i>target-num</i>	ID for the target. This ID is local to the UNIVERGE WL Controller and does not need to correspond to a value on the target itself. You can specify a number from 1 to 10.
<i>ip-addr[:udp-port-number]</i>	IP address of the server. You also can specify the UDP port number to send notifications to.
<i>community-string</i>	Community string.
profile <i>profile-name</i>	Notification profile this SNMP user will use to specify the notification types to send or drop.

retries <i>num</i>	Specifies the number of times the UNIVERGE WL Control System SNMP engine will resend a notification that has not been acknowledged by the target. You can specify from 0 to 3 retries.
timeout <i>num</i>	Specifies the number of seconds UNIVERGE WL Control System waits for acknowledgement of a notification. You can specify from 1 to 5 seconds.

SNMPv2c with Traps

To configure a notification target for traps from SNMPv2c, use the following command:

Syntax **set snmp notify target** *target-num ip-addr[:udp-port-number]*
v2c *community-string* **trap**
[profile *profile-name*]

<i>target-num</i>	ID for the target. This ID is local to the UNIVERGE WL Controller and does not need to correspond to a value on the target itself. You can specify a number from 1 to 10.
<i>ip-addr[:udp-port-number]</i>	IP address of the server. You also can specify the UDP port number to send notifications to.
<i>community-string</i>	Community string.
profile <i>profile-name</i>	Notification profile this SNMP user will use to specify the notification types to send or drop.

set snmp notify target

Chapter 8

SNMPv1 with Traps

To configure a notification target for traps from SNMPv1, use the following command:

Syntax **set snmp notify target** *target-num* *ip-addr[:udp-port-number]*
v1 *community-string*
[profile *profile-name*]

<i>target-num</i>	ID for the target. This ID is local to the UNIVERGE WL Controller and does not need to correspond to a value on the target itself. You can specify a number from 1 to 10.
<i>ip-addr[:udp-port-number]</i>	IP address of the server. You also can specify the UDP port number to send notifications to.
<i>community-string</i>	Community string.
profile <i>profile-name</i>	Notification profile this SNMP user will use to specify the notification types to send or drop.

Defaults The default UDP port number on the target is 162. The default minimum required security level is **unsecured**. The default number of retries is 0 and the default timeout is 2 seconds.

Access Enabled.

Usage The **inform** or **trap** option specifies whether the UNIVERGE WL Control System SNMP engine expects the target to acknowledge notifications sent to the target by the UNIVERGE WL Controller. Use **inform** if you want acknowledgements. Use **trap** if you do not want acknowledgements. The **inform** option is applicable to SNMP version **v2c** or **usm** only.

Examples The following command configures a notification target for acknowledged notifications:

```
PROMPT# set snmp notify target 1 10.10.40.9 usm inform user securesnmppmgr1
      snmp-engine-id ip
success: change accepted.
```

This command configures target 1 at IP address 10.10.40.9. The target SNMP engine ID is based on its address. The UNIVERGE WL Control System SNMP engine sends notifications based on the default profile, and requires the target to acknowledge receiving them.

The following command configures a notification target for unacknowledged notifications:

```
PROMPT# set snmp notify target 2 10.10.40.10 v1 trap
success: change accepted.
```

See Also

- 1 **clear snmp notify target** on page 104
- 1 **set ip snmp server** on page 122
- 1 **set snmp community** on page 130
- 1 **set snmp notify profile** on page 132
- 1 **set snmp protocol** on page 143
- 1 **set snmp security** on page 144
- 1 **set snmp usm** on page 146
- 1 **show snmp notify target** on page 174

set snmp protocol

Enables an SNMP protocol. UNIVERGE WL Control System supports SNMPv1, SNMPv2c, and SNMPv3.

Syntax **set snmp protocol** {**v1** | **v2c** | **usm** | **all**} {**enable** | **disable**}

v1	SNMPv1
v2c	SNMPv2c
usm	SNMPv3 (with the user security model)
all	Enables all supported versions of SNMP.

set snmp security

Chapter 8

enable	Enables the specified SNMP version(s).
disable	Disables the specified SNMP version(s).

Defaults All SNMP versions are disabled by default.

Access Enabled.

Usage SNMP requires the UNIVERGE WL Controller system IP address to be set. SNMP does not work without the system IP address.

You also must enable the SNMP service using the **set ip snmp server** command.

Examples The following command enables all SNMP versions:

```
PROMPT# set snmp protocol all enable
success: change accepted.
```

See Also

- 1 **set ip snmp server** on page 122
- 1 **set snmp community** on page 130
- 1 **set snmp notify target** on page 137
- 1 **set snmp notify profile** on page 132
- 1 **set snmp security** on page 144
- 1 **set snmp usm** on page 146
- 1 **show snmp status** on page 174

set snmp security

Sets the minimum level of security UNIVERGE WL Control System requires for SNMP message exchanges.

Syntax `set snmp security`
{ **unsecured** | **authenticated** | **encrypted** | **auth-req-unsec-notify** }

unsecured	SNMP message exchanges are not secure. This is the only value supported for SNMPv1 and SNMPv2c.
authenticated	SNMP message exchanges are authenticated but are not encrypted.
encrypted	SNMP message exchanges are authenticated and encrypted.
auth-req-unsec-notify	SNMP message exchanges are authenticated but are not encrypted, and notifications are neither authenticated nor encrypted.

Defaults By default, UNIVERGE WL Control System allows nonsecure (**unsecured**) SNMP message exchanges.

Access Enabled.

Usage SNMPv1 and SNMPv2c do not support authentication or encryption. If you plan to use SNMPv1 or SNMPv2c, leave the minimum level of SNMP security set to **unsecured**.

Examples The following command sets the minimum level of SNMP security allowed to authentication *and* encryption:

```
PROMPT# set snmp security encrypted
success: change accepted.
```

See Also

- 1 **set ip snmp server** on page 122
- 1 **set snmp community** on page 130
- 1 **set snmp notify target** on page 137
- 1 **set snmp notify profile** on page 132
- 1 **set snmp protocol** on page 143
- 1 **set snmp usm** on page 146
- 1 **show snmp status** on page 174

set snmp usm

Creates a USM user for SNMPv3.



Note. This command does not apply to SNMPv1 or SNMPv2c. For these SNMP versions, use the **set snmp community** command to configure community strings.

Syntax `set snmp usm usm-username`
`snmp-engine-id {ip ip-addr | local | hex hex-string}`
`access {read-only | read-notify | notify-only | read-write | notify-read-write}`
`auth-type {none | md5 | sha}`
`{auth-pass-phrase string | auth-key hex-string}`
`encrypt-type {none | des | 3des | aes}`
`{encrypt-pass-phrase string | encrypt-key hex-string}`

usm-username

Name of the SNMPv3 user. Specify between 1 and 32 alphanumeric characters, with no spaces.

snmp-engine-id {**ip** *ip-addr* | **local** | **hex** *hex-string*}

Specifies a unique identifier for the SNMP engine.

To send informs, you must specify the engine ID of the inform receiver. To send traps and to allow get and set operations and so on, specify **local** as the engine ID.

- **hex** *hex-string*—ID is a hexadecimal string.
- **ip** *ip-addr*—ID is based on the IP address of the station running the management application. Enter the IP address of the station. UNIVERGE WL Control System calculates the engine ID based on the address.
- **local**—Uses the value computed from the UNIVERGE WL Controllers system IP address.

**access { read-only | read-notify |
notify-only | read-write |
notify-read-write }**

Specifies the access level of the user:

- **read-only**—An SNMP management application using the string can get (read) object values on the UNIVERGE WL Controller but cannot set (write) them.
- **read-notify**—An SNMP management application using the string can get object values on the UNIVERGE WL Controller but cannot set them. The UNIVERGE WL Controller can use the string to send notifications.
- **notify-only**—The UNIVERGE WL Controller can use the string to send notifications.
- **read-write**—An SNMP management application using the string can get and set object values on the UNIVERGE WL Controller.
- **notify-read-write**—An SNMP management application using the string can get and set object values on the UNIVERGE WL Controller. The UNIVERGE WL Controller can use the string to send notifications.

auth-type { **none** | **md5** | **sha** }
{ **auth-pass-phrase** *string* | **auth-key** *hex-string* }

Specifies the authentication type used to authenticate communications with the remote SNMP engine. You can specify one of the following:

- **none**—No authentication is used.
- **md5**—Message-digest algorithm 5 is used.
- **sha**—Secure Hashing Algorithm (SHA) is used.

If the authentication type is **md5** or **sha**, you can specify a passphrase or a hexadecimal key.

- To specify a passphrase, use the **auth-pass-phrase** *string* option. The string can be from 8 to 32 alphanumeric characters long, with no spaces.
- To specify a key, use the **auth-key** *hex-string* option.

encrypt-type { **none** | **des** | **3des** | **aes** }
{encrypt-pass-phrase *string* |
encrypt-key *hex-string* }

Specifies the encryption type used for SNMP traffic. You can specify one of the following:

- **none**—No encryption is used. This is the default.
- **des**—Data Encryption Standard (DES) encryption is used.
- **3des**—Triple DES encryption is used.
- **aes**—Advanced Encryption Standard (AES) encryption is used.

If the encryption type is **des**, **3des**, or **aes**, you can specify a passphrase or a hexadecimal key.

- To specify a passphrase, use the **encrypt-pass-phrase** *string* option. The string can be from 8 to 32 alphanumeric characters long, with no spaces.
- To specify a key, use the **encrypt-key** *hex-string* option.

Defaults No SNMPv3 users are configured by default. When you configure an SNMPv3 user, the default access is **read-only**, and the default authentication and encryption types are both **none**.

Access Enabled.

Examples The following command creates USM user *snmpmgr1*, associated with the local SNMP engine ID. This user can send traps to notification receivers.

```
PROMPT# set snmp usm snmpmgr1 snmp-engine-id local
success: change accepted.
```

The following command creates USM user *securesnmpmgr1*, which uses SHA authentication and 3DES encryption with passphrases. This user can send informs to the notification receiver that has engine ID 192.168.40.2.

```
PROMPT# set snmp usm securesnmpmgr1 snmp-engine-id ip 192.168.40.2 auth-type sha
auth-pass-phrase myauthpassword encrypt-type 3des encrypt-pass-phrase
mycryptpassword
```

success: change accepted.

See Also

- 1 **clear snmp usm** on page 105
- 1 **set ip snmp server** on page 122
- 1 **set snmp community** on page 130
- 1 **set snmp notify target** on page 137
- 1 **set snmp notify profile** on page 132
- 1 **set snmp protocol** on page 143
- 1 **set snmp security** on page 144
- 1 **show snmp usm** on page 175

set summertime

Offsets the real-time clock of a UNIVERGE WL Controller by +1 hour and returns it to standard time for daylight savings time or a similar summertime period.

Syntax **set summertime** *summer-name* [**start** *week weekday month hour min* **end** *week weekday month hour min*]

<i>summer-name</i>	Name of up to 32 alphanumeric characters that describes the summertime offset. You can use a standard name or any name you like. (You cannot use a number as the first character.)
start	Start of the time change period.
<i>week</i>	Week of the month to start or end the time change. Valid values are first , second , third , fourth , or last .
<i>weekday</i>	Day of the week to start or end the time change. Valid values are sun , mon , tue , wed , thu , fri , and sat .
<i>month</i>	Month of the year to start or end the time change. Valid values are jan , feb , mar , apr , may , jun , jul , aug , sep , oct , nov , and dec .

set summertime

Chapter 8

<i>hour</i>	Hour to start or end the time change—a value between 0 and 23 on the 24-hour clock.
<i>min</i>	Minute to start or end the time change—a value between 0 and 59.
end	End of the time change period.

Defaults If you do not specify a start and end time, the system implements the time change starting at 2:00 a.m. on the first Sunday in April and ending at 2:00 a.m. on the last Sunday in October, according to the North American standard.

Access Enabled.

Usage You must first set the time zone with the **set timezone** command for the offset to work properly without the start and end values.

Configure summertime *before* you set the time and date. Otherwise, the summertime adjustment of the time makes the time incorrect, if the date is within the summertime period.

Examples To enable summertime and set the summertime time zone to *PDT* (Pacific Daylight Time), type the following command:

```
Controller# set summertime PDT
success: change accepted
```

See Also

- 1 **clear summertime** on page 105
- 1 **clear timezone** on page 107
- 1 **set timedate** on page 154
- 1 **set timezone** on page 155
- 1 **show summertime** on page 175
- 1 **show timedate** on page 176
- 1 **show timezone** on page 177

set system ip-address

Configures the system IP address. The system IP address determines the interface or source IP address UNIVERGE WL Control System uses for system tasks, including the following:

- 1 Mobility domain operations
- 1 Topology reporting for dual-homed AP
- 1 Default source IP address used in unsolicited communications such as AAA accounting reports and SNMP traps

Syntax `set system ip-address ip-addr`

ip-addr IP address, in dotted decimal notation. The address must be configured on one of the UNIVERGE WL Controller VLANs.

Defaults None.

Access Enabled.

Usage You must use an address that is configured on one of the UNIVERGE WL Controller VLANs.

To display the system IP address, use the **show system** command.

Examples The following commands configure an IP interface on VLAN *taupe* and configure the interface to be the system IP address:

```
PROMPT# set interface taupe ip 10.10.20.20/24
success: set ip address 10.10.20.20 netmask 255.255.255.0 on vlan taupe

PROMPT# set system ip-address 10.10.20.20
success: change accepted.
```

See Also

- 1 **clear system ip-address** on page 106
- 1 **set interface** on page 111
- 1 **show system** on page 40

set timedate

Sets the time of day and date on the UNIVERGE WL Controller.

Syntax `set timedate {date mmm dd yyyy [time hh:mm:ss]}`

date *mmm dd yyyy*

System date:

- *mmm*—month.
- *dd*—day.
- *yyyy*—year.

time *hh:mm:ss*

System time, in hours, minutes, and seconds.

Defaults None.

Access Enabled.

Usage The day of week is automatically calculated from the day that you set. The time displayed by the CLI after you type the command might be slightly later than the time you enter due to the interval between when you press Enter and when the CLI reads and displays the new time and date.

Configure summertime *before* you set the time and date. Otherwise, the summertime adjustment makes the time incorrect, if the date is within the summertime period.

Examples The following command sets the date to March 13, 2003 and time to 11:11:12:

```
PROMPT# set timedate date feb 29 2004 time 23:58:00
Time now is: Sun Feb 29 2004, 23:58:02 PST
```

See Also

- 1 **clear summertime** on page 105
- 1 **clear timezone** on page 107
- 1 **set summertime** on page 151
- 1 **set timezone** on page 155
- 1 **show summertime** on page 175

1 **show timedate** on page 176

1 **show timezone** on page 177

set timezone

Sets the number of hours, and optionally, the number of minutes, that the UNIVERGE WL Controller real-time clock is offset from Coordinated Universal Time (UTC). These values are also used by Network Time Protocol (NTP), if it is enabled.

Syntax **set timezone** *zone-name* {-hours [*minutes*]}

<i>zone-name</i>	Time zone name of up to 32 alphabetic characters. You can use a standard name or any name you like.
-	Minus time to indicate hours (and minutes) to be subtracted from UTC. Otherwise, hours and minutes are added by default.
<i>hours</i>	Number of hours to add or subtract from UTC.
<i>minutes</i>	Number of minutes to add or subtract from UTC.

Defaults If this command is not used, then the default time zone is UTC.

Access Enabled.

Examples To set the time zone for Pacific Standard Time (PST), type the following command:

```
Controller# set timezone PST -8
Timezone is set to 'PST', offset from UTC is -8:0 hours.
```

See Also

1 **clear summertime** on page 105

1 **clear timezone** on page 107

1 **set summertime** on page 151

1 **set timedate** on page 154

1 **show summertime** on page 175

show arp

Chapter 8

1 **show timedate** on page 176

1 **show timezone** on page 177

show arp

Displays the ARP table.

Syntax **show arp** [*ip-addr*]

ip-addr IP address.

Defaults If you do not specify an IP address, the entire ARP table is displayed.

Access All.

Examples The following command displays ARP entries:

```
PROMPT# show arp
ARP aging time: 1200 seconds

Host                HW Address          VLAN  State   Type
-----
10.5.4.51            00:0b:0e:02:76:f5    1     RESOLVED DYNAMIC
10.5.4.53            00:0b:0e:02:76:f7    1     RESOLVED LOCAL
```

Table 13 describes the fields in this display.

Table 13. Output for show arp

Field	Description
ARP aging time	Number of seconds a dynamic entry can remain unused before UNIVERGE WL Control System removes the entry from the ARP table.
Host	IP address, hostname, or alias.
HW Address	MAC address mapped to the IP address, hostname, or alias.
VLAN	VLAN the entry is for.

Table 13. Output for show arp

Field	Description
Type	Entry type: <ul style="list-style-type: none">• DYNAMIC—Entry was learned from network traffic and ages out if unused for longer than the ARP aging timeout.• LOCAL—Entry for the UNIVERGE WL Controller MAC address. Each VLAN has one local entry for the UNIVERGE WL Controller MAC address.• PERMANENT—Entry does not age out and remains in the configuration even following a reboot.• STATIC—Entry does not age out but is removed after a reboot.
State	Entry state: <ul style="list-style-type: none">• RESOLVING—UNIVERGE WL Control System sent an ARP request for the entry and is waiting for the reply.• RESOLVED—Entry is resolved.

See Also

1 **set arp** on page 109

1 **set arp agingtime** on page 110

show dhcp-client

Displays DHCP client information for all VLANs.

Syntax **show dhcp-client**

Defaults None.

Access All.

show dhcp-client

Chapter 8

Examples The following command displays DHCP client information:

```
PROMPT# show dhcp-client
Interface:      corpvlan(4)
Configuration Status: Enabled
DHCP State:     IF_UP
Lease Allocation: 65535 seconds
Lease Remaining: 65532 seconds
IP Address:     10.3.1.110
Subnet Mask:    255.255.255.0
Default Gateway: 10.3.1.1
DHCP Server:    10.3.1.4
DNS Servers:    10.3.1.29
DNS Domain Name: mycorp.com
```

Table 14 describes the fields in this display.

Table 14. Output for show dhcp-client

Field	Description
Interface	VLAN name and number.
Configuration Status	Status of the DHCP client on this VLAN: <ul style="list-style-type: none">• Enabled• Disabled
DHCP State	State of the IP interface: <ul style="list-style-type: none">• IF_UP• IF_DOWN
Lease Allocation	Duration of the address lease.
Lease Remaining	Number of seconds remaining before the address lease expires.
IP Address	IP address received from the DHCP server.
Subnet Mask	Network mask of the IP address received from the DHCP server.
Default Gateway	Default router (gateway) IP address received from the DHCP server. If the address is 0.0.0.0, the server did not provide an address.
DHCP Server	IP address of the DHCP server.

Table 14. Output for show dhcp-client

Field	Description
DNS Servers	DNS server IP address(es) received from the DHCP server.
DNS Domain Name	Default DNS domain name received from the DHCP server.

See Also `set interface dhcp-client` on page 112

show dhcp-server

Displays UNIVERGE WL Control System DHCP server information.

Syntax `show dhcp-server [interface vlan-id] [verbose]`

interface *vlan-id* Displays the IP addresses leased by the specified VLAN.

verbose Displays configuration and status information for the UNIVERGE WL Control System DHCP server.

Defaults None.

Access All.

Examples The following command displays the addresses leased by the UNIVERGE WL Control System DHCP server:

```
PROMPT# show dhcp-server
VLAN Name      Address      MAC          Lease Remaining(sec)
-----
1 default      10.10.20.2   00:01:02:03:04:05   12345
1 default      10.10.20.3   00:01:03:04:06:07   2103
2 red-vlan     192.168.1.5   00:01:03:04:06:08    102
2 red-vlan     192.168.1.7   00:01:03:04:06:09  16789
```

The following command displays configuration and status information for each VLAN on which the DHCP server is configured:

```
PROMPT# show dhcp-server verbose
Interface:      0 (Direct AP)
```

show dhcp-server

Chapter 8

```
Status:                UP
Address Range:         10.0.0.1-10.0.0.253

Interface:             default(1)
Status:                UP
Address Range:         10.10.20.2-10.10.20.254
Hardware Address:      00:01:02:03:04:05
State:                 BOUND
Lease Allocation:      43200 seconds
Lease Remaining:       12345 seconds
IP Address:            10.10.20.2
Subnet Mask:           255.255.255.0
Default Router:        10.10.20.1
DNS Servers:           10.10.20.4 10.10.20.5
DNS Domain Name:       mycorp.com
```

Table 15 and Table 16 describe the fields in these displays.

Table 15. Output for show dhcp-server

Field	Description
VLAN	VLAN number.
Name	VLAN name.
Address	IP address leased by the server.
MAC Address	MAC address of the device that holds the lease for the address.
Lease Remaining	Number of seconds remaining before the address lease expires.

Table 16. Output for show dhcp-server verbose

Field	Description
Interface	VLAN name and number.
Status	Status of the interface: <ul style="list-style-type: none">• UP• DOWN
Address Range	Range from which the server can lease addresses.

Table 16. Output for show dhcp-server verbose

Field	Description
Hardware Address	MAC address of the DHCP client.
State	<p>State of the address lease:</p> <ul style="list-style-type: none"> • SUSPEND—UNIVERGE WL Control System is checking for the presence of another DHCP server on the subnet. This is the initial state of the UNIVERGE WL Control System DHCP server. The UNIVERGE WL Control System DHCP server remains in this state if another DHCP server is detected. • CHECKING—UNIVERGE WL Control System is using ARP to verify whether the address is available. • OFFERING—UNIVERGE WL Control System offered the address to the client and is waiting for the client to send a DHCPREQUEST for the address. • BOUND—The client accepted the address. • HOLDING—The address is already in use and is therefore unavailable.
Lease Allocation	Duration of the address lease, in seconds.
Lease Remaining	Number of seconds remaining before the address lease expires.
IP Address	IP address leased to the client.
Subnet Mask	Network mask of the IP address leased to the client.
Default Router	Default router IP address included in the DHCP Offer to the client.
DNS Servers	DNS server IP address(es) included in the DHCP Offer to the client.
DNS Domain Name	Default DNS domain name included in the DHCP Offer to the client.

See Also `set interface dhcp-server` on page 113

show interface

Displays the IP interfaces configured on the UNIVERGE WL Controller.

show interface

Chapter 8

Syntax `show interface [vlan-id]`

vlan-id VLAN name or number.

Defaults If you do not specify a VLAN ID, interfaces for all VLANs are displayed.

Access All.

Usage The IP interface table flags an address assigned by a DHCP server with an asterisk (*).

Examples The following command displays all the IP interfaces configured on a UNIVERGE WL Controller:

```
PROMPT# show interface
VLAN Name      Address      Mask          Enabled State RIB
-----
1 default      10.10.10.10  255.255.255.0 YES    Up   ipv4
2 mauve        10.10.20.10  255.255.255.0 NO     Down  ipv4
4 corpvlan     *10.3.1.110  255.255.255.0 YES    Up   ipv4
```

Table 17 describes the fields in this display.

Table 17. Output for show interface

Field	Description
VLAN	VLAN number
Name	VLAN name
Address	IP address
Mask	Subnet mask
Enabled	Administrative state: <ul style="list-style-type: none">• YES (enabled)• NO (disabled)
State	Link state: <ul style="list-style-type: none">• Up (operational)• Down (unavailable)
RIB	Routing Information Base

See Also

- 1 **clear interface** on page 97
- 1 **set interface** on page 111
- 1 **set interface status** on page 115

show ip alias

Displays the IP aliases configured on the UNIVERGE WL Controller.

Syntax **show ip alias** [*name*]

name Alias string.

Defaults If you do not specify an alias name, all aliases are displayed.

Access Enabled.

Examples The following command displays all the aliases configured on a UNIVERGE WL Controller:

```
PROMPT# show ip alias
Name                IP Address
-----
HR1                 192.168.1.2
payroll             192.168.1.3
radius1             192.168.7.2
```

Table 18 describes the fields in this display.

Table 18. Output for show ip alias

Field	Description
Name	Alias string.
IP Address	IP address associated with the alias.

See Also

- 1 **clear ip alias** on page 98

- 1 **set ip alias** on page 115

show ip dns

Displays the DNS servers used by the UNIVERGE WL Controller.

Syntax **show ip dns**

Defaults None.

Access All.

Examples The following command displays the DNS information:

```
PROMPT# show ip dns
Domain Name: example.com
DNS Status: enabled
IP Address          Type
-----
10.1.1.1            PRIMARY
10.1.1.2            SECONDARY
10.1.2.1            SECONDARY
```

Table 19 describes the fields in this display.

Table 19. Output for show ip dns

Field	Description
Domain Name	Default domain name configured on the UNIVERGE WL Controller
DNS Status	Status of the UNIVERGE WL Controllers DNS client: <ul style="list-style-type: none">• Enabled• Disabled
IP Address	IP address of the DNS server
Type	Server type: <ul style="list-style-type: none">• PRIMARY• SECONDARY

See Also

- 1 **clear ip dns domain** on page 99
- 1 **clear ip dns server** on page 99
- 1 **set ip dns** on page 116
- 1 **set ip dns domain** on page 117
- 1 **set ip dns server** on page 118

show ip https

Displays information about the HTTPS management port.

Syntax **show ip https**

Defaults None.

Access All.

Examples The following command shows the status and port number for the HTTPS management interface to the UNIVERGE WL Controller:

```
PROMPT> show ip https
HTTPS is enabled
HTTPS is set to use port 443
```

Last 10 Connections:

IP Address	Last Connected	Time Ago (s)
10.10.10.56	2003/05/09 15:51:26 pst	349

Table 20 describes the fields in this display.

Table 20. Output for show ip https

Field	Description
HTTPS is enabled/disabled	State of the HTTPS server: <ul style="list-style-type: none"> • Enabled • Disabled
HTTPS is set to use port	TCP port number on which the UNIVERGE WL Controller listens for HTTPS connections.
Last 10 connections	List of the last 10 devices to establish connections to the UNIVERGE WL Controller HTTPS server.
IP Address	IP address of the device that established the connection. Note: If a browser connects to a UNIVERGE WL Controller from behind a proxy, then only the proxy IP address is shown. If multiple browsers connect using the same proxy, the proxy address appears only once in the output.
Last Connected	Time when the device established the HTTPS connection to the UNIVERGE WL Controller.
Time Ago (s)	Number of seconds since the device established the HTTPS connection to the UNIVERGE WL Controller.

See Also

- 1 **clear ip telnet** on page 101
- 1 **set ip https server** on page 119
- 1 **set ip telnet** on page 125
- 1 **set ip telnet server** on page 126
- 1 **show ip telnet** on page 169

show ip route

Displays the IP route table on the UNIVERGE WL Controller.

Syntax `show ip route` [*destination*]

destination Route destination IP address, in dotted decimal notation.

Defaults None.

Access All.

Usage When you add an IP interface to an available VLAN, UNIVERGE WL Control System adds direct and local routes for the interface to the route table. If the VLAN is down, UNIVERGE WL Control System does not add the routes. If you add an interface to a VLAN but the routes for that interface do not appear in the route table, use the **show vlan config** command to check the VLAN state.

If you add a static route and the route state is shown as Down, use the **show interface** command to verify that the UNIVERGE WL Controller has an IP interface in the default router subnet. UNIVERGE WL Control System cannot resolve a static route unless one of the UNIVERGE WL Controller VLANs has an interface in the default router subnet. If the UNIVERGE WL Controller has such an interface but the static route is still down, use the **show vlan config** command to check the state of the VLAN ports.

Examples The following command shows all routes in a UNIVERGE WL Controller IP route table:

```
PROMPT# show ip route
Router table for IPv4
Destination/Mask  Proto  Metric  NH-Type  Gateway  VLAN:Interface
-----
0.0.0.0/ 0       Static    1 Router  10.0.1.17  Down
0.0.0.0/ 0       Static    2 Router  10.0.2.17  vlan:2:ip
10.0.2.1/24      IP        0 Direct                vlan:2:ip
10.0.2.1/32      IP        0 Direct                vlan:2:ip:10.0.1.1/24
10.0.2.255/32    IP        0 Direct                vlan:2:ip:10.0.1.1/24
224.0.0.0/ 4     IP        0 Local                  MULTICAST
```

Table 21 describes the fields in this display.

Table 21. Output for show ip route

Field	Description
Destination/Mask	IP address and subnet mask of the route destination. The 244.0.0.0 route is automatically added by UNIVERGE WL Control System and supports the IGMP snooping feature.
Proto	Protocol that added the route to the IP route table. The protocol can be one of the following: <ul style="list-style-type: none">• IP—UNIVERGE WL Control System added the route.• Static—An administrator added the route.
Metric	Cost for using the route.
NH-Type	Next-hop type: <ul style="list-style-type: none">• Local—Route is for a local interface. UNIVERGE WL Control System adds the route when you configure an IP address on a UNIVERGE WL Controller.• Direct—Route is for a locally attached subnet. UNIVERGE WL Control System adds the route when you add an interface in the same subnet as the UNIVERGE WL Controller.• Router—Route is for a remote destination. A UNIVERGE WL Controller forwards traffic for the destination to the default router (gateway).

Table 21. Output for show ip route

Field	Description
Gateway	Next-hop router for reaching the route destination. Note: This field applies only to static routes.
VLAN:Interface	Destination VLAN, protocol type, and IP address of the route. Because direct routes are for local interfaces, a destination IP address is not listed. The destination for the IP multicast route is MULTICAST. For static routes, the value Down means the UNIVERGE WL Controller does not have an interface to the destination next-hop router. To provide an interface, configure an IP interface that is in the same IP subnet as the next-hop router. The IP interface must be on a VLAN with the port attached to the default router.

See Also

- 1 **clear ip route** on page 100
- 1 **set interface** on page 111
- 1 **set ip route** on page 120
- 1 **show interface** on page 161
- 1 **show vlan config** on page 86

show ip telnet

Displays information about the Telnet management port.

Syntax **show ip telnet**

Defaults None.

Access All.

show ntp

Chapter 8

Examples The following command shows the status and port number for the Telnet management interface to the UNIVERGE WL Controller:

```
PROMPT> show ip telnet
```

Server Status	Port
Enabled	23

Table 22 describes the fields in this display.

Table 22. Output for show ip telnet

Field	Description
Server Status	State of the HTTPS server: <ul style="list-style-type: none">• Enabled• Disabled
Port	TCP port number on which the UNIVERGE WL Controller listens for Telnet management traffic.

See Also

- 1 **clear ip telnet** on page 101
- 1 **set ip https server** on page 119
- 1 **set ip telnet** on page 125
- 1 **set ip telnet server** on page 126
- 1 **show ip https** on page 165

show ntp

Displays NTP client information.

Syntax `show ntp`

Defaults None.

Access All.

Examples To display NTP information for a UNIVERGE WL Controller, type the following command:

```
PROMPT> show ntp
NTP client: enabled
Current update-interval: 20(secs)
Current time: Fri Feb 06 2004, 12:02:57
Timezone is set to 'PST', offset from UTC is -8:0 hours.
Summertime is enabled.
Last NTP update: Fri Feb 06 2004, 12:02:46
NTP Server      Peer state      Local State
-----
192.168.1.5     SYSPEER          SYNCED
```

Table 23 describes the fields in this display.

Table 23. Output for show ntp

Field	Description
NTP client	State of the NTP client. The state can be one of the following: <ul style="list-style-type: none"> • Enabled • Disabled
Current update-interval	Number of seconds between queries sent by the UNIVERGE WL Controller to the NTP servers for updates.
Current time	System time that was current on the UNIVERGE WL Controller when you pressed Enter after typing the show ntp command.
Timezone	Time zone configured on the UNIVERGE WL Controller. UNIVERGE WL Control System offsets the time reported by the NTP server based on the time zone. <p>Note: This field is displayed only if you change the time zone.</p>

Table 23. Output for show ntp

Field	Description
Summertime	Summertime period configured on the UNIVERGE WL Controller. UNIVERGE WL Control System offsets the system time +1 hour and returns it to standard time for daylight savings time or a similar summertime period that you set. Note: This field is displayed only if you enable summertime.
Last NTP update	Time when the UNIVERGE WL Controller received the most recent update from an NTP server.
NTP Server	IP address of the NTP server.
Peer state	State of the NTP session from the point of view of the NTP server: <ul style="list-style-type: none"> • CORRECT • REJECT • SELCAND • SYNCCAND • SYSPEER
Local state	State of the NTP session on the UNIVERGE WL Controller NTP client: <ul style="list-style-type: none"> • INITED • START • SYNCED

See Also

- 1 **clear ntp server** on page 102
- 1 **clear summertime** on page 105
- 1 **clear timezone** on page 107
- 1 **set ntp** on page 127
- 1 **set ntp server** on page 128

- 1 **set summertime** on page 151
- 1 **set timezone** on page 155
- 1 **show timezone** on page 177

show snmp community

Displays the configured SNMP community strings.

Syntax **show snmp community**

Defaults None.

Access Enabled.

See Also

- 1 **clear snmp community** on page 103
- 1 **set snmp community** on page 130

show snmp counters

Displays SNMP statistics counters.

Syntax **show snmp counters**

Defaults None.

Access Enabled.

show snmp notify profile

Displays SNMP notification profiles.

Syntax **show snmp notify profile**

Defaults None.

Access Enabled.

show snmp notify target

Chapter 8

- 1 **clear snmp notify profile** on page 103
- 1 **set snmp notify profile** on page 132

show snmp notify target

Displays SNMP notification targets.

Syntax **show snmp notify target**

Defaults None.

Access Enabled.

See Also

- 1 **clear snmp notify target** on page 104
- 1 **set snmp notify target** on page 137

show snmp status

Displays SNMP version and status information.

Syntax **show snmp status**

Defaults None.

Access Enabled.

See Also

- 1 **set snmp community** on page 130
- 1 **set snmp notify target** on page 137
- 1 **set snmp notify profile** on page 132
- 1 **set snmp protocol** on page 143
- 1 **set snmp security** on page 144
- 1 **set snmp usm** on page 146

- 1 **show snmp community** on page 173
- 1 **show snmp counters** on page 173
- 1 **show snmp notify profile** on page 173
- 1 **show snmp notify target** on page 174
- 1 **show snmp usm** on page 175

show snmp usm

Displays information about SNMPv3 users.

Defaults None.

Access Enabled.

See Also

- 1 **clear snmp usm** on page 105
- 1 **show snmp usm** on page 175

show summertime

Shows a UNIVERGE WL Controller offset time from its real-time clock time.

Syntax **show summertime**

Defaults There is no summertime offset by default.

Access All.

Examples To display the summertime setting on a UNIVERGE WL Controller, type the following command:

```
Controller# show summertime
Summertime is enabled, and set to 'PDT'.
  Start   : Sun Apr 04 2004, 02:00:00
  End     : Sun Oct 31 2004, 02:00:00
  Offset  : 60 minutes
  Recurring : yes, starting at 2:00 am of first Sunday of April
             and ending at 2:00 am on last Sunday of October.
```

See Also

- 1 **clear summertime** on page 105
- 1 **clear timezone** on page 107
- 1 **set summertime** on page 151
- 1 **set timedate** on page 154
- 1 **set timezone** on page 155
- 1 **show timedate** on page 176
- 1 **show timezone** on page 177

show timedate

Shows the date and time of day currently set on a UNIVERGE WL Controller real-time clock.

Syntax **show timedate**

Defaults None.

Access All.

Examples To display the time and date set on a UNIVERGE WL Controller real-time clock, type the following command:

```
Controller# show timedate
Sun Feb 29 2004, 23:59:02 PST
```

See Also

- 1 **clear summertime** on page 105
- 1 **clear timezone** on page 107
- 1 **set summertime** on page 151
- 1 **set timedate** on page 154
- 1 **set timezone** on page 155
- 1 **show summertime** on page 175

- 1 **show timezone** on page 177

show timezone

Shows the time offset for the real-time clock from UTC on a UNIVERGE WL Controller.

Syntax **show timezone**

Defaults None.

Access All.

Examples To display the offset from UTC, type the following command:

```
PROMPT# show timezone
Timezone set to 'pst', offset from UTC is -8 hours
```

See Also

- 1 **clear summertime** on page 105
- 1 **clear timezone** on page 107
- 1 **set summertime** on page 151
- 1 **set timedate** on page 154
- 1 **set timezone** on page 155
- 1 **show summertime** on page 175
- 1 **show timedate** on page 176

telnet

Opens a Telnet client session with a remote device.

Syntax **telnet** {*ip-addr* | *hostname*} [**port** *port-num*]

ip-addr IP address of the remote device.

telnet

Chapter 8

hostname Hostname of the remote device.

port *port-num* TCP port number on which the TCP server on the remote device listens for Telnet connections.

Defaults UNIVERGE WL Control System attempts to establish Telnet connections with TCP port 23 by default.

Access Enabled.

Usage To end a Telnet session from the remote device, press Ctrl+t or type **exit** in the management session on the remote device. To end a client session from the local device, use the **clear sessions telnet client** command.

If the configuration of the UNIVERGE WL Controller on which you enter the **telnet** command has an ACL that denies Telnet client traffic, the ACL also denies access by the **telnet** command.

Examples In the following example, an administrator establishes a Telnet session with another UNIVERGE WL Controller and enters a command on the remote UNIVERGE WL Controller:

```
PROMPT# telnet 10.10.10.90
Session 0 pty tty2.d Trying 10.10.10.90...
Connected to 10.10.10.90
Disconnect character is '^t'
```

Copyright (c) 2006 NEC Infrontia Corporation. All rights reserved.

```
Username: username
Password: password
```

```
PROMPT-remote> show vlan
      Admin  VLAN  Tunl
VLAN Name  Status State Affin Port   Tag   State
-----
  1 default    Up    Up           5
                   1    none  Up
```

When the administrator presses Ctrl+t to end the Telnet connection, the management session returns to the local UNIVERGE WL Controller prompt:

```
PROMPT-remote> Session 0 pty tty2.d terminated tt name tty2.d
PROMPT#
```

See Also

- 1 **clear sessions** on page 531
- 1 **show sessions** on page 534

tracert

Traces the route from the UNIVERGE WL Controller to an IP host.

Syntax **tracert** *host* [**dnf**] [**no-dns**] [**port** *port-num*] [**queries** *num*]
[**size** *size*] [**ttl** *hops*] [**wait** *ms*]

<i>host</i>	IP address, hostname, or alias of the destination host. Specify the IP address in dotted decimal notation.
dnf	Sets the Do Not Fragment bit in the ping packet to prevent the packet from being fragmented.
no-dns	Prevents UNIVERGE WL Control System from performing a DNS lookup for each hop to the destination host.
port <i>port-num</i>	TCP port number listening for the tracert probes.
queries <i>num</i>	Number of probes per hop.
size <i>size</i>	Probe packet size in bytes. You can specify from 40 through 1460.
ttl <i>hops</i>	Maximum number of hops, which can be from 1 through 255.
wait <i>ms</i>	Probe wait in milliseconds. You can specify from 1 through 100,000.

Defaults

- 1 **dnf**—Disabled
- 1 **no-dns**—Disabled
- 1 **port**—33434
- 1 **queries**—3
- 1 **size**—38

traceroute

Chapter 8

1 **tthl**—30

1 **wait**—5000

Access All.

Usage To stop a **traceroute** command that is in progress, press Ctrl+C.

Examples The following example traces the route to host *server1*:

```
PROMPT# traceroute server1
traceroute to server1.example.com (192.168.22.7), 30 hops max, 38 byte packets
1 engineering-1.example.com (192.168.192.206) 2 ms 1 ms 1 ms
2 engineering-2.example.com (192.168.196.204) 2 ms 3 ms 2 ms
3 gateway_a.example.com (192.168.1.201) 6 ms 3 ms 3 ms
4 server1.example.com (192.168.22.7) 3 ms * 2 ms
```

The first row of the display indicates the target host, the maximum number of hops, and the packet size. Each numbered row displays information about one hop. The rows are displayed in the order that the hops occur, beginning with the hop closest to the UNIVERGE WL Controller.

The row for a hop lists the total time in milliseconds for each ICMP packet to reach the router or host, plus the time for the *ICMP Time Exceeded* message to return to the host.

An exclamation point (!) following any of these values indicates that the *Port Unreachable* message returned by the destination has a maximum hop count of 0 or 1. This can occur if the destination uses the maximum hop count value from the arriving packet as the maximum hop count in its ICMP reply. The reply does not arrive at the source until the destination receives a traceroute packet with a maximum hop count equal to the number of hops between the source and destination.

An asterisk (*) indicates that the timeout period expired before UNIVERGE WL Control System received a *Time Exceeded* message for the packet.

If Traceroute receives an ICMP error message other than a *Time Exceeded* or *Port Unreachable* message, UNIVERGE WL Control System displays one of the error codes described in Table 24 instead of displaying the round-trip time or an asterisk (*).

Table 24 describes the **traceroute** error messages.

Table 24. Error Messages for tracert

Field	Description
!N	No route to host. The network is unreachable.
!H	No route to host. The host is unreachable.
!P	Connection refused. The protocol is unreachable.
!F	Fragmentation needed but Do Not Fragment (DNF) bit was set.
!S	Source route failed.
!A	Communication administratively prohibited.
?	Unknown error occurred.

See Also ping on page 107

AAA Commands

Use authentication, authorization, and accounting (AAA) commands to provide a secure network connection and a record of user activity. Location policy commands override any virtual LAN (VLAN) or security ACL assignment by AAA or the local UNIVERGE WL Controller database to help you control access locally.

(Security ACLs are packet filters. For command descriptions, see Chapter 14, “Security ACL Commands,” on page 453.)

This chapter presents AAA commands alphabetically. Use the following table to locate commands in this chapter based on their use.

Authentication	set authentication console on page 206
	set authentication admin on page 203
	set authentication dot1x on page 209
	set authentication mac on page 213
	set authentication last-resort on page 212
	clear authentication admin on page 186
	clear authentication console on page 187
	clear authentication dot1x on page 188
	clear authentication last-resort on page 189
	clear authentication mac on page 189
	clear authentication web on page 190
Local Authorization for Password Users	set user on page 235
	clear user on page 196
	set user attr on page 236
	clear user attr on page 196

	set usergroup on page 238
	clear usergroup on page 198
	set user group on page 237
	clear user group on page 197
	clear usergroup attr on page 199
Local Authorization for MAC Users	set mac-user on page 221
	clear mac-user on page 191
	set mac-user attr on page 222
	clear mac-user attr on page 192
	set mac-usergroup attr on page 230
	clear mac-usergroup attr on page 194
	clear mac-user group on page 193
	clear mac-usergroup on page 193
Web authorization	set web-portal on page 240
Accounting	set accounting {admin console} on page 200
	set accounting {dot1x mac web last-resort} on page 201
	show accounting statistics on page 243
	clear accounting on page 185
AAA information	show aaa on page 240
Mobility Profiles	set mobility-profile on page 231
	set mobility-profile mode on page 234
	show mobility-profile on page 247
	clear mobility-profile on page 195
Location Policy	set location policy on page 217
	show location policy on page 246
	clear location policy on page 190

clear accounting

Removes accounting services for specified wireless users with administrative access or network access.

Syntax `clear accounting {admin | dot1x | system} {user-glob}`

admin Users with administrative access to the UNIVERGE WL Controller through a console connection or through a Telnet or WebView connection.

dot1x Users with network access through the UNIVERGE WL Controller. Users with network access are authorized to use the network through either an IEEE 802.1X method or their media access control (MAC) address.

system Disables sending of Accounting-On and Accounting-Off messages to a RADIUS server, if previously enabled. When this command is entered, an Accounting-Off message is generated and sent to the server or server group specified with the **set accounting system** command.

user-glob Single user or set of users with administrative access or network access.
Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an *at* sign (@) or a period (.). (For details, see “User Globs” on page 9.)

Defaults None.

Access Enabled.

Examples The following command removes accounting services for authorized network user Nin:

```
PROMPT# clear accounting dot1x Nin
success: change accepted.
```

See Also

1 **set accounting {admin | console}** on page 200

- 1 **show accounting statistics** on page 243

clear authentication admin

Removes an authentication rule for administrative access through Telnet or Web View.

Syntax **clear authentication admin** *user-glob*

user-glob

A single user or set of users.

Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character, either an *at* sign (@) or a period (.). (For details, see “User Globs” on page 9.)

Defaults None.

Access Enabled.



Note. The syntax descriptions for the **clear authentication** commands are separate for clarity. However, the options and behavior for the **clear authentication admin** command are the same as in previous releases.

Examples The following command clears authentication for administrator Jose:

```
PROMPT# clear authentication admin Jose
success: change accepted.
```

See Also

- 1 **clear authentication console** on page 187
- 1 **clear authentication dot1x** on page 188
- 1 **clear location policy** on page 190
- 1 **clear authentication web** on page 190
- 1 **set authentication admin** on page 203

1 **show aaa** on page 240

clear authentication console

Removes an authentication rule for administrative access through the Console.

Syntax **clear authentication console** *user-glob*

<i>user-glob</i>	A single user or set of users. Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character, either an <i>at</i> sign (@) or a period (.). (For details, see “User Globs” on page 9.)
------------------	--

Defaults None.

Access Enabled.



Note. The syntax descriptions for the **clear authentication** commands are separate for clarity. However, the options and behavior for the **clear authentication console** command are the same as in previous releases.

Examples The following command clears authentication for administrator Regina:

```
PROMPT# clear authentication console Regina
success: change accepted.
```

See Also

- 1 **clear authentication admin** on page 186
- 1 **clear authentication dot1x** on page 188
- 1 **clear authentication mac** on page 189
- 1 **clear authentication web** on page 190
- 1 **set authentication console** on page 206

- 1 **show aaa** on page 240

clear authentication dot1x

Removes an 802.1X authentication rule.

Syntax **clear authentication dot1x** {**ssid** *ssid-name*} *user-glob*

ssid SSID name to which this authentication rule applies.
ssid-name

user-glob User-glob associated with the rule you are removing.

Defaults None.

Access Enabled.

Examples The following command removes 802.1X authentication for network users with usernames ending in *@thiscorp.com* who try to access SSID *finance*:

```
PROMPT# clear authentication dot1x ssid finance *@thiscorp.com
```

See Also

- 1 **clear authentication admin** on page 186
- 1 **clear authentication console** on page 187
- 1 **clear authentication mac** on page 189
- 1 **clear authentication web** on page 190
- 1 **set authentication dot1x** on page 209
- 1 **show aaa** on page 240

clear authentication last-resort

Deprecated in WL1700-MS of UNIVERGE WL Control System V1. The *last-resort* user is not required or supported in WL1700-MS of UNIVERGE WL Control System V1. Instead, a user who accesses the network on an SSID by using the fallthru access type **last-resort** is automatically a *last-resort* user. The authorization attributes assigned to the user come from the default authorization attributes set on the SSID.

clear authentication mac

Removes a MAC authentication rule.

Syntax **clear authentication mac** {**ssid** *ssid-name*} *mac-addr-glob*

ssid *ssid-name* SSID name to apply the authentication.

mac-addr-glob MAC address glob associated with the rule you are removing.

Defaults None.

Access Enabled.

Examples The following command removes a MAC authentication rule for access to SSID *thatcorp* by MAC addresses beginning with *aa:bb:cc*:

```
PROMPT# clear authentication mac ssid thatcorp aa:bb:cc:*
```

See Also

- 1 **clear authentication admin** on page 186
- 1 **clear authentication console** on page 187
- 1 **clear authentication dot1x** on page 188
- 1 **clear authentication web** on page 190
- 1 **set authentication mac** on page 213
- 1 **show aaa** on page 240

clear authentication web

Removes a Web Authentication rule.

Syntax **clear authentication web** {**ssid** *ssid-name*} *user-glob*

ssid SSID name to which this authentication rule applies.
ssid-name

user-glob User-glob associated with the rule you are removing.

Defaults None.

Access Enabled.

Examples The following command removes Web Authentication for SSID *research* and userglob *temp*@thiscorp.com*:

```
PROMPT# clear authentication web ssid research temp*@thiscorp.com
```

See Also

- 1 **clear authentication admin** on page 186
- 1 **clear authentication console** on page 187
- 1 **clear authentication dot1x** on page 188
- 1 **clear authentication mac** on page 189
- 1 **set authentication web** on page 215
- 1 **show aaa** on page 240

clear location policy

Removes a rule from the location policy on a UNIVERGE WL Controller.

Syntax **clear location policy** *rule-number*

rule-number Index number of a location policy rule to remove from the location policy.

Defaults None.

Access Enabled.

Usage To determine the index numbers of location policy rules, use the **show location policy** command. Removing all the ACEs from the location policy disables this function on the UNIVERGE WL Controller.

Examples The following command removes location policy rule 4 from a UNIVERGE WL Controller's location policy:

```
PROMPT# clear location policy 4
success: clause 4 is removed.
```

See Also

- 1 **set location policy** on page 217
- 1 **show location policy** on page 246

clear mac-user

Removes a user profile from the local database on the UNIVERGE WL Controller, for a user authenticated by a MAC address.

(To remove a user profile in RADIUS, see the documentation for your RADIUS server.)

Syntax **clear mac-user** *mac-addr*

mac-addr MAC address of the user, in hexadecimal numbers separated by colons (:). You can omit leading zeros.

Defaults None.

Access Enabled.

Usage Deleting a MAC user profile from the database deletes the assignment of any profile attributes to the user.

Examples The following command removes the user profile for a user at MAC address 01:02:03:04:05:06:

```
PROMPT# clear mac-user 01:02:03:04:05:06
success: change accepted.
```

See Also

- 1 **set mac-usergroup attr** on page 230
- 1 **set mac-user attr** on page 222
- 1 **show aaa** on page 240

clear mac-user attr

For a user authenticating with a MAC address, this command removes an authorization attribute from the user profile in the local database on the UNIVERGE WL Controller.

(To remove an authorization attribute in RADIUS, see the documentation for your RADIUS server.)

Syntax **clear mac-user** *mac-addr attr attribute-name*

<i>mac-addr</i>	MAC address of the user, in hexadecimal numbers separated by colons (:). You can omit leading zeros.
<i>attribute-name</i>	Name of an attribute used to authorize the MAC user for a particular service or session characteristic. (For a list of authorization attributes, see Table 25 on page 223.)

Defaults None.

Access Enabled.

Examples The following command removes an access control list (ACL) from the profile of a user at MAC address 01:02:03:04:05:06:

```
PROMPT# clear mac-user 01:02:03:04:05:06 attr filter-id
success: change accepted.
```

See Also

- 1 **set mac-user attr** on page 222
- 1 **show aaa** on page 240

clear mac-user group

Removes a user profile from a MAC user group in the local database on the UNIVERGE WL Controller, for a user authenticating with a MAC address.

(To remove a MAC user group profile in RADIUS, see the documentation for your RADIUS server.)

Syntax `clear mac-user mac-addr group`

mac-addr MAC address of the user, in hexadecimal numbers separated by colons (:). You can omit leading zeros.

Defaults None.

Access Enabled.

Usage Removing a MAC user from a MAC user group removes the group name from the user profile, but does not delete the user group from the local UNIVERGE WL Controller database. To remove the group, use **clear mac-usergroup**.

Examples The following command deletes a user profile at MAC address 01:02:03:04:05:06 from its user group:

```
PROMPT# clear mac-user 01:02:03:04:05:06 group
success: change accepted.
```

See Also

- 1 **clear mac-usergroup** on page 193
- 1 **set mac-user** on page 221
- 1 **show aaa** on page 240

clear mac-usergroup

Removes a user group from the local database on the UNIVERGE WL Controller, for a group of users authenticating with a MAC address.

(To delete a MAC user group in RADIUS, see the documentation for your RADIUS server.)

clear mac-usergroup attr

Chapter 9

Syntax **clear mac-usergroup** *group-name*

group-name Name of an existing MAC user group.

Defaults None.

Access Enabled.

Usage To remove a user from a MAC user group, use the **clear mac-user group** command.

Examples The following command deletes the MAC user group *eastcoasters* from the local database:

```
PROMPT# clear mac-usergroup eastcoasters
success: change accepted.
```

See Also

- 1 **clear mac-usergroup attr** on page 194
- 1 **set mac-usergroup attr** on page 230
- 1 **show aaa** on page 240

clear mac-usergroup attr

Removes an authorization attribute from a MAC user group in the local database on the UNIVERGE WL Controller, for a group of users who are authenticated by a MAC address.

(To unconfigure an authorization attribute in RADIUS, see the documentation for your RADIUS server.)

Syntax **clear mac-usergroup** *group-name attr attribute-name*

group-name Name of an existing MAC user group.

attribute-name Name of an attribute used to authorize the MAC users in the user group for a particular service or session characteristic. (For a list of authorization attributes, see Table 25 on page 223.)

Defaults None.

Access Enabled.

Usage To remove the group itself, use the **clear mac-usergroup** command.

Examples The following command removes the members of the MAC user group *eastcoasters* from a VLAN assignment by deleting the VLAN-Name attribute from the group:

```
PROMPT# clear mac-usergroup eastcoasters attr vlan-name
success: change accepted.
```

See Also

- 1 **clear mac-usergroup** on page 193
- 1 **set mac-usergroup attr** on page 230
- 1 **show aaa** on page 240

clear mobility-profile

Removes a Mobility Profile entirely.

Syntax **clear mobility-profile** *name*

name Name of an existing Mobility Profile.

Defaults None.

Access Enabled.

Examples The following command removes the Mobility Profile for user Nin:

```
PROMPT# clear mobility-profile Nin
success: change accepted.
```

See Also

- 1 **set mobility-profile** on page 231
- 1 **set mobility-profile mode** on page 234
- 1 **show mobility-profile** on page 247

clear user

Removes a user profile from the local database on the UNIVERGE WL Controller, for a user with a password.

(To remove a user profile in RADIUS, see the documentation for your RADIUS server.)

Syntax **clear user** *username*

username Username of a user with a password.

Defaults None.

Access Enabled.

Usage Deleting the user profile from the database deletes the assignment of any profile attributes to the user.

Examples The following command deletes the user profile for user Nin:

```
PROMPT# clear user Nin
success: change accepted.
```

See Also

1 **set user** on page 235

1 **show aaa** on page 240

clear user attr

Removes an authorization attribute from the user profile in the local database on the UNIVERGE WL Controller, for a user with a password.

(To remove an authorization attribute from a RADIUS user profile, see the documentation for your RADIUS server.)

Syntax **clear user** *username* **attr** *attribute-name*

username Username of a user with a password.

attribute-name Name of an attribute used to authorize the user for a particular service or session characteristic. (For a list of authorization attributes, see Table 25 on page 223.)

Defaults None.

Access Enabled.

Examples The following command removes the Session-Timeout attribute from Hosni's user profile:

```
PROMPT# clear user Hosni attr session-timeout
success: change accepted.
```

See Also

1 **set user attr** on page 236

1 **show aaa** on page 240

clear user group

Removes a user with a password from membership in a user group in the local database on the UNIVERGE WL Controller.

(To remove a user from a user group in RADIUS, see the documentation for your RADIUS server.)

Syntax **clear user** *username* **group**

username Username of a user with a password.

Defaults None.

Access Enabled.

Usage Removing the user from the group removes the group name from the user profile, but does not delete either the user or the user group from the local UNIVERGE WL Controller database. To remove the group, use **clear usergroup**.

Examples The following command removes the user Nin from the user group Nin is in:

```
PROMPT# clear user Nin group
success: change accepted.
```

See Also

- 1 **clear usergroup** on page 198
- 1 **set user group** on page 237
- 1 **show aaa** on page 240

clear usergroup

Removes a user group and its attributes from the local database on the UNIVERGE WL Controller, for users with passwords.

(To delete a user group in RADIUS, see the documentation for your RADIUS server.)

Syntax **clear usergroup** *group-name*

group-name Name of an existing user group.

Defaults None.

Access Enabled.

Usage Removing a user group from the local UNIVERGE WL Controller database does not remove the user profiles of the group members from the database.

Examples The following command deletes the *cardiology* user group from the local database:

```
PROMPT# clear usergroup cardiology
success: change accepted.
```

See Also

- 1 **clear usergroup attr** on page 199
- 1 **set usergroup** on page 238
- 1 **show aaa** on page 240

clear usergroup attr

Removes an authorization attribute from a user group in the local database on the UNIVERGE WL Controller.

(To remove an authorization attribute in RADIUS, see the documentation for your RADIUS server.)

Syntax **clear usergroup** *group-name* **attr** *attribute-name*

<i>group-name</i>	Name of an existing user group.
<i>attribute-name</i>	Name of an attribute used to authorize all the users in the group for a particular service or session characteristic. (For a list of authorization attributes, see Table 25 on page 223.)

Defaults None.

Access Enabled.

Examples The following command removes the members of the user group *cardiology* from a network access time restriction by deleting the Time-Of-Day attribute from the group:

```
PROMPT# clear usergroup cardiology attr time-of-day
success: change accepted.
```

See Also

- 1 **clear usergroup** on page 198
- 1 **set usergroup** on page 238
- 1 **show aaa** on page 240

set accounting {admin | console}

Sets up accounting services for specified wireless users with administrative access, and defines the accounting records and where they are sent.

Syntax **set accounting {admin | console}** {*user-glob*} {**start-stop** | **stop-only**} *method1* [*method2*] [*method3*] [*method4*]

admin	Users with administrative access to the UNIVERGE WL Controller through Telnet or WebView.
console	Users with administrative access to the UNIVERGE WL Controller through a console connection.
<i>user-glob</i>	<p>Single user or set of users with administrative access or network access.</p> <p>Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an <i>at</i> sign (@) or a period (.). (For details, see “User Globs” on page 9.)</p> <p>Note: This option does not apply if mac is specified. For mac, specify a <i>mac-addr-glob</i>. (See “MAC Address Globs” on page 10.)</p>
start-stop	Sends accounting records at the start and end of a network session.
stop-only	Sends accounting records only at the end of a network session.

method1
method2
method3
method4

At least one of up to four methods that UNIVERGE WL Control System uses to process accounting records. Specify one or more of the following methods in priority order. If the first method does not succeed, UNIVERGE WL Control System tries the second method, and so on.

A method can be one of the following:

- **local**—Stores accounting records in the local database on the UNIVERGE WL Controller. When the local accounting storage space is full, UNIVERGE WL Control System overwrites older records with new ones.
- *server-group-name*—Stores accounting records on one or more Remote Authentication Dial-In User Service (RADIUS) servers. You can also enter the names of existing RADIUS server groups as methods.

Defaults Accounting is disabled for all users by default.

Access Enabled.

Usage For network users with start-stop accounting whose records are sent to a RADIUS server, UNIVERGE WL Control System sends interim updates to the RADIUS server when the user roams.

Examples The following command issues start-and-stop accounting records at the local UNIVERGE WL Controller database for administrator Natasha, when she accesses the UNIVERGE WL Controller using Telnet or Web View:

```
PROMPT# set accounting admin Natasha start-stop local
success: change accepted.
```

See Also

- 1 **clear accounting** on page 185
- 1 **show accounting statistics** on page 243

set accounting {dot1x | mac | web | last-resort}

Sets up accounting services for specified wireless users with network access, and defines the accounting records and where they are sent.

set accounting {dot1x | mac | web | last-resort}

Chapter 9

Syntax **set accounting {dot1x | mac | web | last-resort} {ssid ssid-name}**
{user-glob | mac-addr-glob} {start-stop | stop-only}
method1 [method2] [method3] [method4]

dot1x	Users with network access through the UNIVERGE WL Controller who are authenticated by 802.1X.
mac	Users with network access through the UNIVERGE WL Controller who are authenticated by MAC authentication
web	Users with network access through the UNIVERGE WL Controller who are authenticated by Web Authentication
ssid <i>ssid-name</i>	SSID name to which this accounting rule applies. To apply the rule to all SSIDs, type any .
<i>user-glob</i>	Single user or set of users with administrative access or network access. Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an <i>at</i> sign (@) or a period (.). (For details, see “User Globs” on page 9.)
<i>mac-addr-glob</i>	Note: This option does not apply if mac or last-resort is specified. For mac , specify a <i>mac-addr-glob</i> . A single user or set of users with access via a MAC address. Specify a MAC address, or use the wildcard (*) character to specify a set of MAC addresses. (For details, see “MAC Address Globs” on page 10.) This option applies only when mac is specified.
start-stop	Sends accounting records at the start and end of a network session.

stop-only	Sends accounting records only at the end of a network session.
<i>method1</i>	At least one of up to four methods that UNIVERGE WL Control System uses to process accounting records. Specify one or more of the following methods in priority order. If the first method does not succeed, UNIVERGE WL Control System tries the second method, and so on. A method can be one of the following:
<i>method2</i>	
<i>method3</i>	
<i>method4</i>	
	<ul style="list-style-type: none"> • local—Stores accounting records in the local database on the UNIVERGE WL Controller. When the local accounting storage space is full, UNIVERGE WL Control System overwrites older records with new ones. • <i>server-group-name</i>—Stores accounting records on one or more Remote Authentication Dial-In User Service (RADIUS) servers. You can also enter the names of existing RADIUS server groups as methods.

Defaults Accounting is disabled for all users by default.

Access Enabled.

Usage For network users with start-stop accounting profiles whose records are sent to a RADIUS server, UNIVERGE WL Control System sends interim updates to the RADIUS server when the user roams.

Examples The following command issues stop-only records to the RADIUS server group *sg2* for network user *Nin*, who is authenticated by 802.1X:

```
PROMPT# set accounting dot1x Nin stop-only sg2
success: change accepted.
```

See Also

- 1 **clear accounting** on page 185
- 1 **show accounting statistics** on page 243

set authentication admin

Configures authentication and defines where it is performed for specified users with administrative access through Telnet or Web View.

Syntax **set authentication admin** *user-glob*
method1 [*method2*] [*method3*] [*method4*]

user-glob

Single user or set of users with administrative access over the network through Telnet or Web View.

Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an *at* sign (@) or a period (.). (For details, see “User Globs” on page 9.)

method1

method2

method3

method4

At least one of up to four methods that UNIVERGE WL Control System uses to handle authentication. Specify one or more of the following methods in priority order. UNIVERGE WL Control System applies multiple methods in the order you enter them.

A method can be one of the following:

- **local**—Uses the local database of usernames and user groups on the UNIVERGE WL Controller for authentication.
- *server-group-name*—Uses the defined group of RADIUS servers for authentication. You can enter up to four names of existing RADIUS server groups as methods.
- **none**—*For users with administrative access only*, UNIVERGE WL Control System performs no authentication, but prompts for a username and password and accepts any combination of entries, including blanks.

Note: The authentication method **none** you can specify for administrative access is different from the fallthru authentication type **none**, which applies only to network access. The authentication method **none** allows access to the UNIVERGE WL Controller by an administrator. The fallthru authentication type **none** denies access to a network user. (See “set service-profile auth-fallthru” on page 337.)

For more information, see “Usage.”

Defaults By default, authentication is deactivated for all admin users. The default authentication method in an admin authentication rule is **local**. UNIVERGE WL Control System checks the local UNIVERGE WL Controller database for authentication.

Access Enabled.



Note. The syntax descriptions for the **set authentication** commands are separated for clarity. However, the options and behavior for the **set authentication admin** command are the same as in previous releases.

Usage You can configure different authentication methods for different groups of users. (For details, see “User Globs, MAC Address Globs, and VLAN Globs” on page 9.)

If you specify multiple authentication methods in the **set authentication console** command, UNIVERGE WL Control System applies them in the order that they appear in the command, with these results:

- 1 If the first method responds with pass or fail, the evaluation is final.
- 1 If the first method does not respond, UNIVERGE WL Control System tries the second method, and so on.
- 1 However, if **local** appears first, followed by a RADIUS server group, UNIVERGE WL Control System ignores any failed searches in the local UNIVERGE WL Controller database and sends an authentication request to the RADIUS server group.



Note. If a AAA rule specifies local as a secondary AAA method, to be used if the RADIUS servers are unavailable, and UNIVERGE WL Control System authenticates a client with the local method, UNIVERGE WL Control System starts again at the beginning of the method list when attempting to authorize the client. This can cause unexpected delays during client processing and can cause the client to time out before completing logon.

Examples The following command configures administrator Jose, who connects via Telnet, for authentication on RADIUS server group *sg3*:

```
PROMPT# set authentication admin Jose sg3
success: change accepted.
```

See Also

- 1 **clear authentication admin** on page 186
- 1 **set authentication console** on page 206
- 1 **set authentication dot1x** on page 209
- 1 **set authentication mac** on page 213
- 1 **set authentication web** on page 215
- 1 **show aaa** on page 240

set authentication console

Configures authentication and defines where it is performed for specified users with administrative access through a console connection.

Syntax **set authentication console** *user-glob*
method1 [*method2*] [*method3*] [*method4*]

user-glob

Single user or set of users with administrative access through the UNIVERGE WL Controller's console.

Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an *at* sign (@) or a period (.). (For details, see “User Globs” on page 9.)

method1
method2
method3
method4

At least one of up to four methods that UNIVERGE WL Control System uses to handle authentication. Specify one or more of the following methods in priority order. UNIVERGE WL Control System applies multiple methods in the order you enter them.

A method can be one of the following:

- **local**—Uses the local database of usernames and user groups on the UNIVERGE WL Controller for authentication.
- *server-group-name*—Uses the defined group of RADIUS servers for authentication. You can enter up to four names of existing RADIUS server groups as methods.
- **none**—*For users with administrative access only*, UNIVERGE WL Control System performs no authentication, but prompts for a username and password and accepts any combination of entries, including blanks.

Note: The authentication method **none** you can specify for administrative access is different from the fallthru authentication type **none**, which applies only to network access. The authentication method **none** allows access to the UNIVERGE WL Controller by an administrator. The fallthru authentication type **none** denies access to a network user. (See “set service-profile auth-fallthru” on page 337.)

For more information, see “Usage.”

Defaults By default, authentication is deactivated for all console users, and the default authentication method in a console authentication rule is **none**. UNIVERGE WL Control System requires no username or password, by default. These users can press Enter at the prompts for administrative access.



Note. It is recommended that you change the default setting unless the UNIVERGE WL Controller is in a secure physical location.

set authentication console

Chapter 9

Access Enabled..



Note. The syntax descriptions for the **set authentication** commands are separated for clarity. However, the options and behavior for the **set authentication console** command are the same as in previous releases.

Usage You can configure different authentication methods for different groups of users. (For details, see “User Globs, MAC Address Globs, and VLAN Globs” on page 9.)

If you specify multiple authentication methods in the **set authentication console** command, UNIVERGE WL Control System applies them in the order in which they appear in the command, with these results:

- 1 If the first method responds with pass or fail, the evaluation is final.
- 1 If the first method does not respond, UNIVERGE WL Control System tries the second method, and so on.
- 1 However, if **local** appears first, followed by a RADIUS server group, UNIVERGE WL Control System ignores any failed searches in the local UNIVERGE WL Controller database and sends an authentication request to the RADIUS server group.

Examples To set the console port so that it does *not* enforce username-password authentication for administrators, type the following command:

```
PROMPT# set authentication console * none
success: change accepted.
```

See Also

- 1 **clear authentication console** on page 187
- 1 **set authentication admin** on page 203
- 1 **set authentication dot1x** on page 209
- 1 **set authentication mac** on page 213
- 1 **set authentication web** on page 215
- 1 **show aaa** on page 240

set authentication dot1x

Configures authentication and defines how it is performed for specified wireless authentication clients who use an IEEE 802.1X authentication protocol to access the network through the UNIVERGE WL Controller.

Syntax `set authentication dot1x {ssid ssid-name} user-glob [bonded] protocol method1 [method2] [method3] [method4]`

ssid <i>ssid-name</i>	SSID name to which this authentication rule applies. To apply the rule to all SSIDs, type any .
<i>user-glob</i>	A single user or a set of users with 802.1X network access. Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an <i>at</i> sign (@) or a period (.). (For details, see “User Globbs” on page 9.)
bonded	Enables Bonded Auth™ (bonded authentication). When this feature is enabled, UNIVERGE WL Control System authenticates the user only if the computer that the user is on has already been authenticated.

<i>protocol</i>	<p>Protocol used for authentication. Specify one of the following:</p> <ul style="list-style-type: none"> • eap-tls—EAP with Transport Layer Security (TLS): <ul style="list-style-type: none"> • Provides mutual authentication, integrity-protected negotiation, and key exchange • Requires X.509 public key certificates on both sides of the connection • Provides encryption and integrity checking for the connection • Cannot be used with RADIUS server authentication (requires user information to be in the UNIVERGE WL Controller local database) • peap-mschapv2—Protected EAP (PEAP) with Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP-V2). <i>For wireless clients:</i> <ul style="list-style-type: none"> • Uses TLS for encryption and data integrity checking and server-side authentication • Provides MS-CHAP-V2 mutual authentication • Only the server side of the connection needs a certificate. <p>The wireless client authenticates using TLS to set up an encrypted session. Then MS-CHAP-V2 performs mutual authentication using the specified AAA method.</p> • pass-through—UNIVERGE WL Control System sends all the EAP protocol processing to a RADIUS server.
<i>method1</i>	<p>At least one and up to four methods that UNIVERGE WL Control System uses to handle authentication. Specify one or more of the following methods in priority order. UNIVERGE WL Control System applies multiple methods in the order you enter them.</p> <p>A method can be one of the following:</p> <ul style="list-style-type: none"> • local—Uses the local database of usernames and user groups on the UNIVERGE WL Controller for authentication. • <i>server-group-name</i>—Uses the defined group of RADIUS servers for authentication. You can enter up to four names of existing RADIUS server groups as methods. <p>RADIUS servers cannot be used with the EAP-TLS protocol.</p> <p>For more information, see “Usage.”</p>
<i>method2</i>	
<i>method3</i>	
<i>method4</i>	

Defaults By default, authentication is unconfigured for all clients on the UNIVERGE WL Controller. Connection, authorization, and accounting are also disabled for these users.

Bonded authentication is disabled by default.

Access Enabled.

Usage You can configure different authentication methods for different groups of users by “globbing.” (For details, see “User Globs” on page 9.)

You can configure a rule either for wireless access to an SSID. If the rule is for wireless access to an SSID, specify the SSID name or specify any to match on all SSID names.

You cannot configure client authentication that uses both EAP-TLS protocol and one or more RADIUS servers. EAP-TLS authentication is supported only on the local UNIVERGE WL Controller database.

If you specify multiple authentication methods in the **set authentication dot1x** command, UNIVERGE WL Control System applies them in the order in which they appear in the command, with these results:

- 1 If the first method responds with pass or fail, the evaluation is final.
- 1 If the first method does not respond, UNIVERGE WL Control System tries the second method, and so on.
- 1 However, if **local** appears first, followed by a RADIUS server group, UNIVERGE WL Control System overrides any failed searches in the local UNIVERGE WL Controller database and sends an authentication request to the server group.

If the user does not support 802.1X, UNIVERGE WL Control System attempts to perform MAC authentication for the user. In this case, if the UNIVERGE WL Controller configuration contains a **set authentication mac** command that matches the SSID the user is attempting to access and the user MAC address, UNIVERGE WL Control System uses the method specified by the command. Otherwise, UNIVERGE WL Control System uses local MAC authentication by default.

set authentication last-resort

Chapter 9

If the username does not match an authentication rule for the SSID the user is attempting to access, UNIVERGE WL Control System uses the *fallthru* authentication type configured for the SSID, which can be **last-resort**, **web-portal** (for Web Authentication), or **none**.

Examples The following command configures EAP-TLS authentication in the local UNIVERGE WL Controller database for SSID *mycorp* and 802.1X client Geetha:

```
PROMPT# set authentication dot1x ssid mycorp Geetha eap-tls local
success: change accepted.
```

The following command configures PEAP-MS-CHAP-V2 authentication at RADIUS server groups *sg1* through *sg3* for all 802.1X clients at *example.com* who want to access SSID *examplecorp*:

```
PROMPT# set authentication dot1x ssid examplecorp *@example.com peap-mschapv2
sg1 sg2 sg3
success: change accepted.
```

See Also

- 1 **clear authentication dot1x** on page 188
- 1 **set authentication admin** on page 203
- 1 **set authentication console** on page 206
- 1 **set authentication mac** on page 213
- 1 **set authentication web** on page 215
- 1 **set service-profile auth-fallthru** on page 337
- 1 **show aaa** on page 240

set authentication last-resort

Deprecated in WL1700-MS of UNIVERGE WL Control System V1. The *last-resort* user is not required or supported in WL1700-MS of UNIVERGE WL Control System V1. Instead, a user who accesses the network on an SSID by using the fallthru access type **last-resort** is automatically a *last-resort* user. The authorization attributes assigned to the user come from the default authorization attributes set on the SSID.

set authentication mac

Configures authentication and defines where it is performed for specified non-802.1X users with network access through a media access control (MAC) address.

Syntax `set authentication mac {ssid ssid-name} mac-addr-glob method1 [method2] [method3] [method4]`

ssid <i>ssid-name</i>	SSID name to which this authentication rule applies. To apply the rule to all SSIDs, type any .
<i>mac-addr-glob</i>	A single user or set of users with access via a MAC address. Specify a MAC address, or use the wildcard (*) character to specify a set of MAC addresses. (For details, see “MAC Address Globs” on page 10.)
<i>method1</i>	At least one of up to four methods that UNIVERGE WL Control System uses to handle authentication. Specify one or more of the following methods in priority order. UNIVERGE WL Control System applies multiple methods in the order you enter them. A method can be one of the following:
<i>method2</i>	
<i>method3</i>	
<i>method4</i>	
	<ul style="list-style-type: none"> • local—Uses the local database of usernames and user groups on the UNIVERGE WL Controller for authentication. • <i>server-group-name</i>—Uses the defined group of RADIUS servers for authentication. You can enter up to four names of existing RADIUS server groups as methods. <p>For more information, see “Usage.”</p>

Defaults By default, authentication is deactivated for all MAC users, which means MAC address authentication fails by default.

Access Enabled.

Usage You can configure different authentication methods for different groups of MAC addresses by “globbing.” (For details, see “User Globs, MAC Address Globs, and VLAN Globs” on page 9.)

If you specify multiple authentication methods in the **set authentication mac** command, UNIVERGE WL Control System applies them in the order in which they appear in the command, with these results:

- 1 If the first method responds with pass or fail, the evaluation is final.
- 1 If the first method does not respond, UNIVERGE WL Control System tries the second method, and so on.
- 1 However, if **local** appears first, followed by a RADIUS server group, UNIVERGE WL Control System ignores any failed searches in the local UNIVERGE WL Controller database and sends an authentication request to the RADIUS server group.

If the UNIVERGE WL Controller configuration contains a **set authentication mac** command that matches the SSID the user is attempting to access and the user MAC address, UNIVERGE WL Control System uses the method specified by the command. Otherwise, UNIVERGE WL Control System uses local MAC authentication by default.

If the username does not match an authentication rule for the SSID the user is attempting to access, UNIVERGE WL Control System uses the *fallthru* authentication type configured for the SSID, which can be **last-resort**, **web-portal** (for Web Authentication), or **none**.

Examples To use the local UNIVERGE WL Controller database to authenticate all users who access the *mycorp2* SSID by their MAC address, type the following command:

```
PROMPT# set authentication ssid mycorp2 mac ** local
success: change accepted.
```

See Also

- 1 **clear authentication mac** on page 189
- 1 **set authentication admin** on page 203
- 1 **set authentication console** on page 206
- 1 **set authentication dot1x** on page 209
- 1 **set authentication web** on page 215
- 1 **show aaa** on page 240

set authentication web

Configures an authentication rule that allows a user to log into the network using a web page served by the UNIVERGE WL Controller. The rule can be activated if the user is not otherwise granted or denied access by 802.1X, or granted access by MAC authentication.

Syntax **set authentication web** {**ssid** *ssid-name*} *user-glob*
method1 [*method2*] [*method3*] [*method4*]

<i>user-glob</i>	<p>A single user or a set of users.</p> <p>Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an <i>at</i> sign (@) or a period (.). (For details, see “User Globs” on page 9.)</p>
ssid <i>ssid-name</i>	<p>SSID name to which this authentication rule applies. To apply the rule to all SSIDs, type any.</p>
<i>method1</i> <i>method2</i> <i>method3</i> <i>method4</i>	<p>At least one and up to four methods that UNIVERGE WL Control System uses to handle authentication. Specify one or more of the following methods in priority order. UNIVERGE WL Control System applies multiple methods in the order you enter them.</p> <p>A method can be one of the following:</p> <ul style="list-style-type: none"> • local—Uses the local database of usernames and user groups on the UNIVERGE WL Controller for authentication. • <i>server-group-name</i>—Uses the defined group of RADIUS servers for authentication. You can enter up to four names of existing RADIUS server groups as methods. <p>RADIUS servers cannot be used with the EAP-TLS protocol.</p> <p>For more information, see “Usage.”</p>

Defaults By default, authentication is unconfigured for all clients on the UNIVERGE WL Controller. Connection, authorization, and accounting are also disabled for these users.

Access Enabled.

Usage You can configure different authentication methods for different groups of users by “globbing.” (For details, see “User Globs” on page 9.)

set authentication web

Chapter 9

You can configure a rule either for wireless access to an SSID. If the rule is for wireless access to an SSID, specify the SSID name or specify **any** to match on all SSID names.

If you specify multiple authentication methods in the **set authentication web** command, UNIVERGE WL Control System applies them in the order in which they appear in the command, with these results:

- 1 If the first method responds with pass or fail, the evaluation is final.
- 1 If the first method does not respond, UNIVERGE WL Control System tries the second method, and so on.
- 1 However, if **local** appears first, followed by a RADIUS server group, UNIVERGE WL Control System overrides any failed searches in the local UNIVERGE WL Controller database and sends an authentication request to the server group.

UNIVERGE WL Control System uses a Web Authentication rule only under the following conditions:

- 1 The client is not denied access by 802.1X or does not support 802.1X.
- 1 The client MAC address does not match a MAC authentication rule.
- 1 The fallthru type is **web-portal**. (For a wireless authentication rule, the fallthru type is specified by the **set service-profile auth-fallthru** command.)

Examples The following command configures a Web Authentication rule in the local UNIVERGE WL Controller database for SSID *ourcorp* and userglob *rnd**:

```
PROMPT# set authentication web ssid ourcorp rnd* local
success: change accepted.
```

See Also

- 1 **clear authentication web** on page 190
- 1 **set authentication admin** on page 203
- 1 **set authentication console** on page 206
- 1 **set authentication dot1x** on page 209
- 1 **show aaa** on page 240

set location policy

Creates and enables a location policy on a UNIVERGE WL Controller. A location policy enables you to locally set or change authorization attributes for a user after the user is authorized by AAA, without making changes to the AAA server.

Syntax **set location policy deny if** {**ssid** *operator ssid-name* | **vlan** *operator vlan-glob* | **user** *operator user-glob* | **port** *port-list* | **ap** *ap-num*} [**before** *rule-number* | **modify** *rule-number*]

Syntax **set location policy permit** {**vlan** *vlan-name* | **inac1** *inac1-name* | **outac1** *outac1-name*} **if** {**ssid** *operator ssid-name* | **vlan** *operator vlan-glob* | **user** *operator user-glob* | **port** *port-list* | **ap** *ap-num*} [**before** *rule-number* | **modify** *rule-number*]

deny Denies access to the network to users with attributes that match the location policy rule.

permit Allows access to the network or to a specified VLAN, and/or assigns a particular security ACL to users with attributes matching the location policy rule.

Action options—For a permit rule, UNIVERGE WL Control System changes the attributes assigned to the user to the values specified by the following options:

vlan *vlan-name* Name of an existing VLAN to assign to users with attributes matching the location policy rule.

inac1 *inac1-name* Name of an existing security ACL to apply to packets *sent to* the UNIVERGE WL Controller with attributes matching the location policy rule.

Optionally, you can add the suffix **.in** to the name.

outac1 *outac1-name* Name of an existing security ACL to apply to packets *sent from* the UNIVERGE WL Controller with characteristics that match the location policy rule.

Optionally, you can add the suffix **.out** to the name.

Condition options—UNIVERGE WL Control System takes the action specified by the rule if all conditions in the rule are met. You can specify one or more of the following conditions:

ssid operator <i>ssid-name</i>	<p>SSID with which the user is associated. The <i>operator</i> must be eq, which applies the location policy rule to all users associated with the SSID.</p> <p>Asterisks (wildcards) are not supported in SSID names. You must specify the complete SSID name.</p>
vlan operator <i>vlan-glob</i>	<p>VLAN-Name attribute assigned by AAA and condition that determines if the location policy rule applies. Replace <i>operator</i> with one of the following operands:</p> <ul style="list-style-type: none"> • eq—Applies the location policy rule to all users assigned VLAN names matching <i>vlan-glob</i>. • neq—Applies the location policy rule to all users assigned VLAN names <i>not</i> matching <i>vlan-glob</i>. <p>For <i>vlan-glob</i>, specify a VLAN name, use the double-asterisk wildcard character (**) to specify all VLAN names, or use the single-asterisk wildcard character (*) to specify a set of VLAN names up to or following the first delimiter character, either an <i>at</i> sign (@) or a period (.). (For details, see “VLAN Glob” on page 10.)</p>
user operator <i>user-glob</i>	<p>Username and condition that determines if the location policy rule applies. Replace <i>operator</i> with one of the following operands:</p> <ul style="list-style-type: none"> • eq—Applies the location policy rule to all usernames matching <i>user-glob</i>. • neq—Applies the location policy rule to all usernames <i>not</i> matching <i>user-glob</i>. <p>For <i>user-glob</i>, specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character, either an <i>at</i> sign (@) or a period (.). (For details, see “User Glob” on page 9.)</p>
before <i>rule-number</i>	<p>Inserts the new location policy rule in front of another rule in the location policy. Specify the number of the existing location policy rule. (To determine the number, use the show location policy command.)</p>

modify <i>rule-number</i>	Replaces the rule in the location policy with the new rule. Specify the number of the existing location policy rule. (To determine the number, use the show location policy command.)
port <i>port-list</i>	List of physical port(s) that determines if the location policy rule applies.

Defaults By default, users are permitted VLAN access and assigned security ACLs according to the VLAN-Name and Filter-Id attributes applied to the users during normal authentication and authorization.

Access Enabled.

Usage Only a single location policy is allowed per UNIVERGE WL Controller. The location policy can contain up to 150 rules. Once configured, the location policy becomes effective immediately. To disable location policy operation, use the **clear location policy** command.

Conditions within a rule are AND'ed. All conditions in the rule must match in order for UNIVERGE WL Control System to take the specified action. If the location policy contains multiple rules, UNIVERGE WL Control System compares the user information to the rules one at a time, in the order the rules appear in the UNIVERGE WL Controller configuration file, beginning with the rule at the top of the list. UNIVERGE WL Control System continues comparing until a user matches all conditions in a rule or until there are no more rules.

The order of rules in the location policy is important to ensure users are properly granted or denied access. To position rules within the location policy, use **before rule-number** and **modify rule-number** in the **set location policy** command, and the **clear location policy rule-number** command.

When applying security ACLs:

- 1 Use **inac1** *inac1-name* to filter traffic that enters the UNIVERGE WL Controller from the network via a network port.
- 1 Use **outac1** *outac1-name* to filter traffic sent from the UNIVERGE WL Controller from the network via a network port.
- 1 You can optionally add the suffixes **.in** and **.out** to *inac1-name* and *outac1-name* so that they match the names of security ACLs stored in the local UNIVERGE WL Controller database.

set location policy

Chapter 9

Examples The following command denies network access to all users at *.theirfirm.com, causing them to fail authorization:

```
PROMPT# set location policy deny if user eq *.theirfirm.com
```

The following command authorizes access to the *guest_1* VLAN for all users who are not at *.wodefirm.com:

```
PROMPT# set location policy permit vlan guest_1 if user neq *.wodefirm.com
```

The following command authorizes users at *.ny.ourfirm.com to access the *bld4.tac* VLAN instead, and applies the security ACL *tac_24* to the traffic they receive:

```
PROMPT# set location policy permit vlan bld4.tac outacl tac_24 if user eq  
*.ny.ourfirm.com
```

The following command authorizes access to users on VLANs with names matching *bld4.** and applies security ACLs *svcs_2* to the traffic they send and *svcs_3* to the traffic they receive:

```
PROMPT# set location policy permit inacl svcs_2 outacl svcs_3 if vlan eq bldg4.*
```

The following command authorizes users entering the network on UNIVERGE WL Controller port 1 to use the *floor2* VLAN, overriding any settings from AAA:

```
PROMPT# set location policy permit vlan floor2 if port 1
```

The following command places all users who are authorized for SSID *tempvendor_a* into VLAN *kiosk_1*:

```
PROMPT# set location policy permit vlan kiosk_1 if ssid eq tempvendor_a  
success: change accepted.
```

See Also

- 1 **clear location policy** on page 190
- 1 **show location policy** on page 246

set mac-user

Configures a user profile in the local database on the UNIVERGE WL Controller for a user who can authenticate by a MAC address, and optionally adds the user to a MAC user group.

(To configure a MAC user profile in RADIUS, see the documentation for your RADIUS server.)

Syntax `set mac-user mac-addr [group group-name]`

mac-addr MAC address of the user, in hexadecimal numbers separated by colons (:). You can omit leading zeros.

group-name Name of an existing MAC user group.

Defaults None.

Access Enabled.

Usage UNIVERGE WL Control System does not require MAC users to belong to user groups.

Users authenticated by MAC address are authenticated only for network access through the UNIVERGE WL Controller. UNIVERGE WL Control System does not support passwords for MAC users.

Examples The following command creates a user profile for a user at MAC address 01:02:03:04:05:06 and assigns the user to the *eastcoasters* user group:

```
PROMPT# set mac-user 01:02:03:04:05:06 group eastcoasters
success: change accepted.
```

See Also

- 1 **clear mac-user** on page 191
- 1 **show aaa** on page 240

set mac-user attr

Assigns an authorization attribute in the local database on the UNIVERGE WL Controller to a user authenticating with a MAC address.

(To assign authorization attributes through RADIUS, see the documentation for your RADIUS server.)

Syntax **set mac-user** *mac-addr* **attr** *attribute-name value*

<i>mac-addr</i>	MAC address of the user, in hexadecimal numbers separated by colons (:). You can omit leading zeros.
<i>attribute-name value</i>	Name and value of an attribute used to authorize the MAC user for a particular service or session characteristic. For a list of authorization attributes and values that you can assign to local users, see Table 25 on page 223.

Defaults None.

Access Enabled.

Usage To change the value of an attribute, enter **set mac-user attr** with the new value. To delete an attribute, use **clear mac-user attr**.

You can assign attributes to individual MAC users and to MAC user groups. If attributes are configured for a MAC user and also for the group the MAC user is in, the attributes assigned to the individual MAC user take precedence for that user. For example, if the start-date attribute configured for a MAC user is earlier than the start-date configured for the MAC user group for the user, the MAC user network access can begin as soon as the user start-date. The MAC user does not need to wait for the MAC user group start date.

Table 25. Authentication Attributes for Local Users

Attribute	Description	Valid Value(s)
encryption-type	<p>Type of encryption required for access by the client. Clients who attempt to use an unauthorized encryption method are rejected.</p> <p>Note: Encryption-Type is a UNIVERGE WL Control System vendor-specific attribute (VSA). The vendor ID is 14525, and the vendor type is 3.</p>	<p>One of the following numbers that identifies an encryption algorithm:</p> <ul style="list-style-type: none"> • 1—AES_CCM (Advanced Encryption Standard using Counter with CBC-MAC) • 2—Reserved • 4—TKIP (Temporal Key Integrity Protocol) • 8—WEP_104 (the default) (Wired-Equivalent Privacy protocol using 104 bits of key strength) • 16—WEP_40 (Wired-Equivalent Privacy protocol using 40 bits of key strength) • 32—NONE (no encryption) • 64—Static WEP <p>In addition to these values, you can specify a sum of them for a combination of allowed encryption types. For example, to specify WEP_104 and WEP_40, use 24.</p>
end-date	Date and time after which the user is no longer allowed to be on the network.	<p>Date and time, in the following format: YY/MM/DD-HH:MM</p> <p>You can use end-date alone or with start-date. You also can use start-date, end-date, or both in conjunction with time-of-day.</p>

Table 25. Authentication Attributes for Local Users

Attribute	Description	Valid Value(s)
filter-id (network access mode only)	Security access control list (ACL), to permit or deny traffic received (input) or sent (output) by the UNIVERGE WL Controller. (For more information about security ACLs, see Chapter 14, “Security ACL Commands,” on page 453.)	Name of an existing security ACL, up to 32 alphanumeric characters, with no tabs or spaces. <ul style="list-style-type: none"> Use <i>acl-name.in</i> to filter traffic that enters the UNIVERGE WL Controller from the network via a network port. Use <i>acl-name.out</i> to filter traffic sent from the UNIVERGE WL Controller from the network via a network port. <p>Note: If the Filter-Id value returned through the authentication and authorization process does not match the name of a committed security ACL in the UNIVERGE WL Controller, the user fails authorization and is unable to authenticate.</p>
idle-timeout	This option is not implemented in the current UNIVERGE WL Control System version.	
mobility-profile (network access mode only)	Mobility Profile attribute for the user. (For more information, see set mobility-profile on page 231.) Note: Mobility-Profile is a UNIVERGE WL Control System vendor-specific attribute (VSA). The vendor ID is 14525, and the vendor type is 2.	Name of an existing Mobility Profile, which can be up to 32 alphanumeric characters, with no tabs or spaces. Note: If the Mobility Profile feature is enabled, and a user is assigned the name of a Mobility Profile that does not exist on the UNIVERGE WL Controller, the user is denied access.

Table 25. Authentication Attributes for Local Users

Attribute	Description	Valid Value(s)
service-type	Type of access the user is requesting.	<p>One of the following numbers:</p> <ul style="list-style-type: none"> • 2—Framed; for network user access • 6—Administrative; for administrative access to the UNIVERGE WL Controller, with authorization to access the enabled (configuration) mode. The user must enter the enable command and the correct enable password to access the enabled mode. • 7—NAS-Prompt; for administrative access to the nonenabled mode only. In this mode, the user can still enter the enable command and the correct enable password to access the enabled mode. <p>For administrative sessions, the UNIVERGE WL Controller always sends 6 (Administrative).</p> <p>The RADIUS server can reply with one of the values listed above.</p> <p>If the service-type is not set on the RADIUS server, administrative users receive NAS-Prompt access, and network users receive Framed access.</p>
session-timeout (network access mode only)	Maximum number of seconds for the user's session.	<p>Number between 0 and 2,147,483,647 seconds (approximately 68.1 years).</p> <p>Note. If the global reauthentication timeout (set by the set dot1x reauth-period command) is shorter than the session-timeout, UNIVERGE WL Control System uses the global timeout instead.</p>
ssid (network access mode only)	SSID the user is allowed to access after authentication.	<p>Name of the SSID you want the user to use. The SSID must be configured in a service profile, and the service profile must be used by a radio profile assigned in the Mobility Domain.</p>

Table 25. Authentication Attributes for Local Users

Attribute	Description	Valid Value(s)
start-date	Date and time at which the user becomes eligible to access the network. UNIVERGE WL Control System does not authenticate the user unless the attempt to access the network occurs at or after the specified date and time, but before the end-date (if specified).	Date and time, in the following format: YY/MM/DD-HH:MM You can use start-date alone or with end-date . You also can use start-date , end-date , or both in conjunction with time-of-day .

Table 25. Authentication Attributes for Local Users

Attribute	Description	Valid Value(s)
time-of-day (network access mode only)	<p>Day(s) and time(s) during which the user is permitted to log into the network.</p> <p>After authorization, the user's session can last until either the Time-Of-Day range or the Session-Timeout duration (if set) expires, whichever is shorter.</p> <p>Note: Time-Of-Day is a UNIVERGE WL Control System vendor-specific attribute (VSA). The vendor ID is 14525, and the vendor type is 4.</p>	<p>One of the following:</p> <ul style="list-style-type: none"> • never—Access is always denied. • any—Access is always allowed. • al—Access is always allowed. • One or more ranges of values that consist of one of the following day designations (required), and a time range in <i>hhmm-hhmm</i> 4-digit 24-hour format (optional): <ul style="list-style-type: none"> • mo—Monday • tu—Tuesday • we—Wednesday • th—Thursday • fr—Friday • sa—Saturday • su—Sunday • wk—Any day between Monday and Friday <p>Separate values or a series of ranges (except time ranges) with commas (,) or a vertical bar (). Do not use spaces.</p> <p>The maximum number of characters is 253.</p> <p>For example, to allow access only on Tuesdays and Thursdays between 10 a.m. and 4 p.m., specify the following: time-of-day tu1000-1600,th1000-1600</p>

Table 25. Authentication Attributes for Local Users

Attribute	Description	Valid Value(s)
time-of-day (network access mode only) (cont.)		<p>To allow access only on weekdays between 9 a.m and 5 p.m., and on Saturdays from 10 p.m. until 2 a.m., specify the following: time-of-day wk0900-1700,sa2200-0200</p> <p>(Also see the examples for set user attr on page 236.)</p> <p>Note: You can use time-of-day in conjunction with start-date, end-date, or both.</p>
url (network access mode only)	URL to which the user is redirected after successful Web Authentication.	<p>Web URL, in standard format. For example: http://www.example.com</p> <p>Note: You must include the <i>http://</i> portion.</p> <p>You can dynamically include any of the variables in the URL string:</p> <ul style="list-style-type: none"> • \$u—Username • \$v—VLAN • \$s—SSID • \$p—Service profile name <p>To use the literal character \$ or ?, use the following:</p> <ul style="list-style-type: none"> • \$\$ • \$q

Table 25. Authentication Attributes for Local Users

Attribute	Description	Valid Value(s)
vlan-name (network access mode only)	<p>Virtual LAN (VLAN) assignment.</p> <p>Note: VLAN-Name is a UNIVERGE WL Control System vendor-specific attribute (VSA). The vendor ID is 14525, and the vendor type is 1.</p> <p>Note: On some RADIUS servers, you might need to use the standard RADIUS attribute Tunnel-Pvt-Group-ID, instead of VLAN-Name.</p>	<p>Name of a VLAN that you want the user to use. The VLAN must be configured on a UNIVERGE WL Controller within the Mobility Domain to which this UNIVERGE WL Controller belongs.</p>
acct-interim-interval	<p>Interval in seconds between accounting updates, if start-stop accounting mode is enabled.</p>	<p>Number between 180 and 3,600 seconds, or 0 to disable periodic accounting updates.</p> <p>The UNIVERGE WL Controller ignores the acct-interim-interval value and issues a log message if the value is below 60 seconds.</p> <p>Note: If both a RADIUS server and the UNIVERGE WL Controller supply a value for the acct-interim-interval attribute, then the value from the UNIVERGE WL Controller takes precedence.</p>

Examples The following command assigns input access control list (ACL) *acl-03* to filter packets from a user at MAC address 01:02:03:04:05:06:

```
PROMPT# set mac-user 01:02:03:04:05:06 attr filter-id acl-03.in
success: change accepted.
```

set mac-usergroup attr

Chapter 9

The following command restricts a user at MAC address 06:05:04:03:02:01 to network access between 7 p.m. on Mondays and Wednesdays and 7 a.m. on Tuesdays and Thursdays:

```
PROMPT# set mac-user 06:05:04:03:02:01 attr time-of-day  
mo1900-1159,tu0000-0700,we1900-1159,th0000-0700  
success: change accepted.
```

See Also

- 1 **clear mac-user attr** on page 192
- 1 **show aaa** on page 240

set mac-usergroup attr

Creates a user group in the local database on the UNIVERGE WL Controller for users authenticated by a MAC address, and assigns authorization attributes for the group.

(To configure a user group and assign authorization attributes through RADIUS, see the documentation for your RADIUS server.)

Syntax **set mac-usergroup** *group-name* **attr** *attribute-name value*

<i>group-name</i>	Name of a MAC user group. Specify a name of up to 32 alphanumeric characters, with no spaces. The name must begin with an alphabetic character.
<i>attribute-name value</i>	Name and value of an attribute used to authorize all MAC users in the group for a particular service or session characteristic. (For a list of authorization attributes, see Table 25 on page 223.)

Defaults None.

Access Enabled.

Usage To change the value of an attribute, enter **set mac-usergroup attr** with the new value. To delete an attribute, use **clear mac-usergroup attr**.

You can assign attributes to individual MAC users and to MAC user groups. If attributes are configured for a MAC user and also for the group of the MAC user, the attributes assigned to the individual MAC user take precedence for that user. For example, if the start-date attribute configured for a MAC user is earlier than the start-date configured for the MAC user group, the MAC user network access can begin as soon as the user start-date. The MAC user does not need to wait for the MAC user group start date.

Examples The following command creates the MAC user group *eastcoasters* and assigns the group members to VLAN *orange*:

```
PROMPT# set mac-usergroup eastcoasters attr vlan-name orange
success: change accepted.
```

See Also

1 **clear mac-usergroup attr** on page 194

1 **show aaa** on page 240

set mobility-profile

Creates a Mobility Profile and specifies the UNIVERGE WL Access Point on the UNIVERGE WL Controller through which any user assigned to the profile is allowed access.

Syntax **set mobility-profile name** *name*
{**ap** {**none** | **all** | *ap-num*}}

name Name of the Mobility Profile. Specify up to 32 alphanumeric characters, with no spaces.

none Prevents any user to whom this profile is assigned from accessing any UNIVERGE WL Access Point on the UNIVERGE WL Controller.

set mobility-profile

Chapter 9

all	Allows any user to whom this profile is assigned to access all UNIVERGE WL Access Points on the UNIVERGE WL Controller.
<i>ap-num</i>	List of UNIVERGE WL Access Points connections through which any user assigned this profile is allowed access. The same UNIVERGE WL Access Points can be used in multiple Mobility Profile port lists.

Defaults No default Mobility Profile exists on the UNIVERGE WL Controller. If you do not assign Mobility Profile attributes, all users have access through all ports, unless denied access by other AAA servers or by access control lists (ACLs).

Access Enabled.

Usage To assign a Mobility Profile to a user or group, specify it as an authorization attribute in one of the following commands:

- 1 **set user attr mobility-profile** *name*
- 1 **set usergroup attr mobility-profile** *name*
- 1 **set mac-user attr mobility-profile** *name*
- 1 **set mac-usergroup attr mobility-profile** *name*

To enable the use of the Mobility Profile feature on the UNIVERGE WL Controller, use the **set mobility-profile mode** command.



Caution! When the Mobility Profile feature is enabled, a user is denied access if assigned a Mobility-Profile attribute in the local UNIVERGE WL Controller database or RADIUS server when no Mobility Profile of that name exists on the UNIVERGE WL Controller.

To change the ports in a profile, use **set mobility-profile** again with the updated port list.

Examples The following commands create the Mobility Profile *magnolia*, which restricts user access to ap 2; enable the Mobility Profile feature on the UNIVERGE WL Controller; and assign the *magnolia* Mobility Profile to user *Jose*.

```
PROMPT# set mobility-profile name magnolia ap 2
success: change accepted.

PROMPT# set mobility-profile mode enable
success: change accepted.

PROMPT# set user Jose attr mobility-profile magnolia
success: change accepted.
```

The following command adds ap 3 to the *magnolia* Mobility Profile (which is already assigned to port 12):

```
PROMPT# set mobility-profile name magnolia ap 2-3
success: change accepted.
```

See Also

- 1 **clear mobility-profile** on page 195
- 1 **set mac-user attr** on page 222
- 1 **set mac-usergroup attr** on page 230
- 1 **set mobility-profile mode** on page 234
- 1 **set user attr** on page 236
- 1 **set usergroup** on page 238
- 1 **show mobility-profile** on page 247

set mobility-profile mode

Enables or disables the Mobility Profile feature on the UNIVERGE WL Controller.



Caution! When the Mobility Profile feature is enabled, a user is denied access if assigned a Mobility-Profile attribute in the local UNIVERGE WL Controller database or RADIUS server if no Mobility Profile of that name exists on the UNIVERGE WL Controller.

Syntax **set mobility-profile mode {enable | disable}**

enable Enables the use of the Mobility Profile feature on the UNIVERGE WL Controller.

disable Specifies that all Mobility Profile attributes are ignored by the UNIVERGE WL Controller.

Defaults The Mobility Profile feature is disabled by default.

Access Enabled.

Examples To enable the use of the Mobility Profile feature, type the following command:

```
PROMPT# set mobility-profile mode enable
success: change accepted.
```

See Also

- 1 **clear mobility-profile** on page 195
- 1 **set mobility-profile** on page 231
- 1 **show mobility-profile** on page 247

set user

Configures a user profile in the local database on the UNIVERGE WL Controller for a user with a password.

(To configure a user profile in RADIUS, see the documentation for your RADIUS server.)

Syntax `set user username password [encrypted] string`

<i>username</i>	Username of a user with a password.
encrypted	Indicates that the password string you entered is already in its encrypted form. If you use this option, UNIVERGE WL Control System does not encrypt the displayed form of the password string, and instead displays the string exactly as you entered it. If you omit this option, UNIVERGE WL Control System does encrypt the displayed form of the string.
password <i>string</i>	Password of up to 38 alphanumeric characters, with no spaces.

Defaults None.

Access Enabled.

Usage The **show config** command shows the **encrypted** option with this command, even when you omit the option. The **encrypted** option appears in the configuration because UNIVERGE WL Control System automatically encrypts the password when you create the user (unless you use the **encrypted** option when you enter the password).

Although UNIVERGE WL Control System allows you to configure a user password for the special “last-resort” guest user, the password has no effect. Last-resort users can never access a UNIVERGE WL Controller in administrative mode and never require a password.

The only valid username of the form *last-resort-** is *last-resort-wired*. The *last-resort-wired* user allows last-resort access on a wired authentication port.

Examples The following command creates a user profile for user Nin in the local database, and assigns the password *goody*:

```
PROMPT# set user Nin password goody
success: User Nin created
```

The following command assigns the password *chey3nne* to the **admin** user:

```
PROMPT# set user admin password chey3nne
success: User admin created
```

The following command changes the password for Nin from *goody* to *29Jan04*:

```
PROMPT# set user Nin password 29Jan04
```

See Also

- 1 **clear user** on page 196
- 1 **show aaa** on page 240

set user attr

Configures an authorization attribute in the local database on the UNIVERGE WL Controller for a user with a password.

(To assign authorization attributes in RADIUS, see the documentation for your RADIUS server.)

Syntax **set user** *username* **attr** *attribute-name value*

<i>username</i>	Username of a user with a password.
<i>attribute-name value</i>	Name and value of an attribute you are using to authorize the user for a particular service or session characteristic. For a list of authorization attributes and values that you can assign to network users, see Table 25 on page 223.

Defaults None.

Access Enabled.

Usage To change the value of an attribute, enter **set user attr** with the new value. To delete an attribute, use **clear user attr**.

You can assign attributes to individual users and to user groups. If attributes are configured for a user and also for the group the user belongs, the attributes assigned to the individual user take precedence for that user. For example, if the start-date attribute configured for a user is earlier than the start-date configured for the user group the user is in, the user has network access as soon as the user start-date. The user does not need to wait for the user group start date.

Examples The following command assigns user Tamara to VLAN *orange*:

```
PROMPT# set user Tamara attr vlan-name orange
success: change accepted.
```

The following command assigns Tamara to the Mobility Profile *tulip*.

```
PROMPT# set user Tamara attr mobility-profile tulip
success: change accepted.
```

The following command limits the days and times when user Student1 can access the network, to 5 p.m. to 2 a.m. every weekday, and all day Saturday and Sunday:

```
PROMPT# set user Student1 attr time-of-day Wk1700-0200,Sa,Su
success: change accepted.
```

See Also

- 1 **clear user attr** on page 196
- 1 **show aaa** on page 240

set user group

Adds a user to a user group. The user must have a password and a profile that exists in the local database on the UNIVERGE WL Controller.

(To configure a user in RADIUS, see the documentation for your RADIUS server.)

set usergroup

Chapter 9

Syntax **set user** *username* **group** *group-name*

username Username of a user with a password.

group-name Name of an existing user group for password users.

Defaults None.

Access Enabled.

Usage UNIVERGE WL Control System does not require users to belong to user groups.

To *create* a user group, use the command **set usergroup**.

Examples The following command adds user Hosni to the *cardiology* user group:

```
PROMPT# set user Hosni group cardiology
success: change accepted.
```

See Also

1 **clear user group** on page 197

1 **show aaa** on page 240

set usergroup

Creates a user group in the local database on the UNIVERGE WL Controller for users and assigns authorization attributes for the group.

(To create user groups and assign authorization attributes in RADIUS, see the documentation for your RADIUS server.)

Syntax **set usergroup** *group-name* **attr** *attribute-name value*

<i>group-name</i>	Name of a group for password users. Specify a name of up to 32 alphanumeric characters, with no spaces. The name must begin with an alphabetic character.
<i>attribute-name value</i>	Name and value of an attribute you are using to authorize all users in the group for a particular service or session characteristic. For a list of authorization attributes and values that you can assign to users, see Table 25 on page 223.

Defaults None.

Access Enabled.

Usage To change the value of an attribute, enter **set usergroup attr** with the new value. To delete an attribute, use **clear usergroup attr**.

To *add* a user to a group, user the command **set user group**.

You can assign attributes to individual users and to user groups. If attributes are configured for a user and also for the group the user belongs, the attributes assigned to the individual user take precedence for that user. For example, if the start-date attribute configured for a user is earlier than the start-date configured for the user group the user belongs, network access for the user can begin as soon as the user start-date. The user does not need to wait for the user group start date.

Examples The following command adds the user group *cardiology* to the local database and assigns all the group members to VLAN *crimson*:

```
PROMPT# set usergroup cardiology attr vlan-name crimson
success: change accepted.
```

See Also

- 1 **clear usergroup** on page 198
- 1 **clear usergroup attr** on page 199
- 1 **show aaa** on page 240

set web-portal

Globally enables or disables Web Authentication on a UNIVERGE WL Controller.

Syntax **set web-portal** {**enable** | **disable**}

enable Enables Web Authentication on the UNIVERGE WL Controller.

disable Disables Web Authentication on the UNIVERGE WL Controller.

Defaults Enabled.

Access Enabled.

Usage This command disables or reenables support for Web Authentication. However, Web Authentication has additional configuration requirements. For information, see the “Configuring AAA for Network Users” chapter in the [Configuration Guide](#).

Examples To disable Web Authentication, type the following command:

```
PROMPT# set web-portal disable
success: change accepted.
```

See Also

- 1 **clear authentication web** on page 190
- 1 **set service-profile auth-fallthru** on page 337
- 1 **set user** on page 235

show aaa

Displays all current AAA settings.

Syntax **show aaa**

Defaults None.

Access Enabled.

Examples To display all current AAA settings, type the following command:

PROMPT# show aaa

Default Values

authport=1812 acctport=1813 timeout=5 acct-timeout=5
retrans=3 deadtime=0 key=(null) author-pass=(null)

Radius Servers

Server	Addr	Ports	T/o	Tries	Dead	State
rs-3	198.162.1.1	1821 1813	5	3	0	UP
rs-4	198.168.1.2	1821 1813	77	11	2	UP
rs-5	198.162.1.3	1821 1813	42	23	0	UP

Server groups

sg1: rs-3

sg2: rs-4

sg3: rs-5

Web Portal:

enabled

```
set authentication admin Jose sg3
set authentication mac ssid mycorp * local
set authentication dotlx ssid mycorp Geetha eap-tls
set authentication dotlx ssid mycorp * peap-mschapv2 sg1 sg2 sg3
set authentication dotlx ssid any ** peap-mschapv2 sg1 sg2 sg3
set accounting dotlx Nin ssid mycorp stop-only sg2
set accounting admin Natasha start-stop local
```

user Nin

Password = 082c6c64060b (encrypted)

Filter-Id = acl-999.in

Filter-Id = acl-999.out

mac-user 01:02:03:04:05:06

usergroup eastcoasters

session-timeout = 99

Table 26 describes the fields that can appear in **show aaa** output.

Table 26. show aaa Output

Field	Description
Default Values	RADIUS default values for all parameters.
authport	UDP port on the UNIVERGE WL Controller for transmission of RADIUS authorization and authentication messages. The default port is 1812.
acctport	UDP port on the UNIVERGE WL Controller for transmission of RADIUS accounting records. The default is port 1813.
timeout	Number of seconds the UNIVERGE WL Controller waits for a RADIUS server to respond before retransmitting. The default is 5 seconds.
acct-timeout	Number of seconds the UNIVERGE WL Controller waits for a RADIUS server to respond to an accounting request before retransmitting. The default is 5 seconds.
retrans	Number of times the UNIVERGE WL Controller retransmits a message before determining a RADIUS server unresponsive. The default is 3 times.
deadtime	Number of minutes the UNIVERGE WL Controller waits after determining a RADIUS server is unresponsive before trying to reconnect with this server. During the dead time, the RADIUS server is ignored by the UNIVERGE WL Controller. The default is 0 minutes.
key	Shared secret key, or password, used to authenticate to a RADIUS server. The default is no key (null).
author-pass	Password used for authorization to a RADIUS server for MAC authentication. The client MAC address is sent as the username and the author-pass string is sent as the password.
Radius Servers	Information about active RADIUS servers.
Server	Name of each RADIUS server currently active.
Addr	IP address of each RADIUS server currently active.
Ports	UDP ports that the UNIVERGE WL Controller uses for authentication messages and for accounting records.
T/o	Setting of timeouts on each RADIUS server currently active.

Table 26. show aaa Output

Field	Description
Tries	Number of retransmissions configured for each RADIUS server currently active. The default is 3 times.
Dead	Length of time until the server is considered responsive again.
State	Current state of each RADIUS server currently active: <ul style="list-style-type: none"> • UP (operating) • DOWN (unavailable)
Server groups	Names of RADIUS server groups and member servers configured on the UNIVERGE WL Controller.
Web Portal	State of the Web Authentication feature: <ul style="list-style-type: none"> • enabled • disabled
set commands	List of commands used to configure AAA on the UNIVERGE WL Controller.
user and user group profiles	List of user and user group profiles stored in the local database on the UNIVERGE WL Controller.

See Also

- 1 **set accounting {admin | console}** on page 200
- 1 **set authentication admin** on page 203
- 1 **set authentication console** on page 206
- 1 **set authentication dot1x** on page 209
- 1 **set authentication mac** on page 213
- 1 **set authentication web** on page 215

show accounting statistics

Displays the AAA accounting records for wireless users. The records are stored in the local database on the UNIVERGE WL Controller.

show accounting statistics

Chapter 9

(To display RADIUS accounting records, see the documentation for your RADIUS server.)

Syntax **show accounting statistics**

Defaults None.

Access Enabled.

Examples To display the locally stored accounting records, type the following command:

```
PROMPT# show accounting statistics
Dec 14 00:39:48
Acct-Status-Type=STOP
Acct-Authentic=0
Acct-Multi-Session-Id=SESS-3-01f82f-520236-24bb1223
Acct-Session-Id=SESS-3-01f82f-520236-24bb1223
User-Name=vineet
AAA_ACCT_SVC_ATTR=2
Acct-Session-Time=551
Event-Timestamp=1134520788
Acct-Output-Octets=3204
Acct-Input-Octets=1691
Acct-Output-Packets=20
Acct-Input-Packets=19
AAA_VLAN_NAME_ATTR=default
Calling-Station-Id=00-60-B9-12-06-38
Nas-Port-Id=3/1
Called-Station-Id=00-60-B9-00-CC-01
AAA_SSID_ATTR=vineet-dot1x

Dec 14 00:39:53
Acct-Status-Type=START
Acct-Authentic=0
User-Name=vineet
Acct-Multi-Session-Id=SESS-4-01f82f-520793-bd779517
Acct-Session-Id=SESS-4-01f82f-520793-bd779517
Event-Timestamp=1134520793
AAA_ACCT_SVC_ATTR=2
AAA_VLAN_NAME_ATTR=default
Calling-Station-Id=00-60-B9-12-06-38
Nas-Port-Id=3/1
Called-Station-Id=00-60-B9-00-CC-01
AAA_SSID_ATTR=vineet-dot1x
```

Table 27 describes the fields that can appear in **show accounting statistics** output.

Table 27. show accounting statistics Output

Field	Description
Date and time	Date and time of the accounting record.
Acct-Status-Type	Type of accounting record: <ul style="list-style-type: none"> • START • STOP • UPDATE
Acct-Authentic	Location where the user was authenticated (if authentication took place) for the session: <ul style="list-style-type: none"> • 1—RADIUS server • 2—Local UNIVERGE WL Controller database
User-Name	Username of a user with a password.
Acct-Multi-Session-Id	Unique accounting ID for multiple related sessions in a log file.
AAA_TTY_ATTR	For sessions conducted through a console or administrative Telnet connection, the Telnet terminal number.
Event-Timestamp	Time (in seconds since January 1, 1970) at which the event was triggered. (See RFC 2869 for more information.)
Acct-Session-Time	Number of seconds that the session has been online.
Acct-Output-Octets	Number of octets the UNIVERGE WL Controller sent during the session.
Acct-Input-Octets	Number of octets the UNIVERGE WL Controller received during the session.
Acct-Output-Packets	Number of packets the UNIVERGE WL Controller sent during the session.
Acct-Input-Packets	Number of packets the UNIVERGE WL Controller received during the session.
Vlan-Name	Name of the client VLAN.
Calling-Station-Id	MAC address of the supplicant (client).

Table 27. show accounting statistics Output

Field	Description
Nas-Port-Id	Number of the port and radio on the UNIVERGE WL Access Points through which the session was conducted.
Called-Station-Id	MAC address of the UNIVERGE WL Access Points through which the client reached the network.

See Also

- 1 **clear accounting** on page 185
- 1 **set accounting {admin | console}** on page 200
- 1 **show aaa** on page 240

show location policy

Displays the list of location policy rules that make up the location policy on a UNIVERGE WL Controller.

Syntax **show location policy**

Defaults None.

Access Enabled.

Examples The following command displays the list of location policy rules in the location policy on a UNIVERGE WL Controller:

```
PROMPT# show location policy
Id Clauses
-----
1) deny if user eq *.theirfirm.com
2) permit vlan guest_1 if vlan neq *.wodefirm.com
3) permit vlan bld4.tac inacl tac_24.in if user eq *.ny.wodefirm.com
```

See Also

- 1 **clear location policy** on page 190
- 1 **set location policy** on page 217

show mobility-profile

Displays the named Mobility Profile. If you do not specify a Mobility Profile name, this command shows all Mobility Profile names and port lists on the UNIVERGE WL Controller.

Syntax `show mobility-profile [name]`

name Name of an existing Mobility Profile.

Defaults None.

Access Enabled.

Examples The following command displays the Mobility Profile *magnolia*:

```
PROMPT# show mobility-profile magnolia
Mobility Profiles
Name                      Ports
=====
magnolia                  AP 2
```

See Also

- 1 **clear mobility-profile** on page 195
- 1 **set mobility-profile** on page 231

show mobility-profile
Chapter 9

Mobility Domain Commands

Use Mobility Domain commands to configure and manage Mobility Domain groups.

A Mobility Domain is a system of UNIVERGE WL Controllers and UNIVERGE WL Access Points working together to support a roaming user (client). One UNIVERGE WL Controller acts as a seed UNIVERGE WL Controller, which maintains and distributes a list of IP addresses of the domain members.



Note. UNIVERGE WL Control System recommends that you run the same UNIVERGE WL Control System version on all the UNIVERGE WL Controllers in a Mobility Domain.

Note. on all the UNIVERGE WL Controllers in a Mobility Domain.

This chapter presents Mobility Domain commands alphabetically. Use the following table to locate commands in this chapter based on their use.

Mobility Domain	set mobility-domain mode seed domain-name on page 253
	set mobility-domain member on page 251
	set mobility-domain mode member seed-ip on page 252
	show mobility-domain on page 254
	show mobility-domain config on page 254
	clear mobility-domain member on page 250
	clear mobility-domain on page 250

clear mobility-domain

Clears all Mobility Domain configuration and information from a UNIVERGE WL Controller, regardless of whether the UNIVERGE WL Controller is a seed or a member of a Mobility Domain.

Syntax **clear mobility-domain**

Defaults None.

Access Enabled.

Usage This command has no effect if the UNIVERGE WL Controller is not configured as part of a Mobility Domain.

Examples To clear a Mobility Domain from a UNIVERGE WL Controller within the domain, type the following command:

```
Controller# clear mobility-domain
success: change accepted.
```

See Also

- 1 **clear mobility-domain member** on page 250
- 1 **set mobility-domain member** on page 251
- 1 **set mobility-domain mode member seed-ip** on page 252
- 1 **set mobility-domain mode seed domain-name** on page 253

clear mobility-domain member

On the seed, the command removes the identified member from the Mobility Domain.

Syntax **clear mobility-domain member** *ip-addr*

ip-addr IP address of the Mobility Domain member, in dotted decimal notation.

Defaults None.

Access Enabled.

Usage This command has no effect if the UNIVERGE WL Controller member is not configured as part of a Mobility Domain or the current UNIVERGE WL Controller is not the seed.

Examples The following command clears a Mobility Domain member with the IP address 192.168.0.1:

```
Controller# clear mobility-domain member 192.168.0.1
```

See Also `set mobility-domain member` on page 251

set mobility-domain member

On the seed UNIVERGE WL Controller, adds a member to the list of Mobility Domain members. If the current UNIVERGE WL Controller is not configured as a seed, this command is rejected.

Syntax `set mobility-domain member ip-addr [key hex-bytes]`

<i>ip-addr</i>	IP address of the Mobility Domain member in dotted decimal notation.
key <i>hex-bytes</i>	Fingerprint of the public key to use for UNIVERGE WL Controller-UNIVERGE WL Controller security. Specify the key as 16 hexadecimal bytes. Use a colon between each byte, as in the following example: 00:11:22:33:44:55:66:77:88:99:aa:bb:cc:dd:ee:ff

Defaults None.

Access Enabled.

Usage This command must be entered from the seed UNIVERGE WL Controller .

Examples The following commands add three UNIVERGE WL Controllers with the IP addresses 192.168.1.8, 192.168.1.9, and 192.168.1.10 as members of a Mobility Domain whose seed is the current UNIVERGE WL Controller:

```
PROMPT# set mobility-domain member 192.168.1.8
```

set mobility-domain mode member seed-ip

Chapter 10

```
success: change accepted.  
PROMPT# set mobility-domain member 192.168.1.9  
success: change accepted.  
PROMPT# set mobility-domain member 192.168.1.10  
success: change accepted.
```

See Also

- 1 **clear mobility-domain member** on page 250
- 1 **set mobility-domain mode seed domain-name** on page 253
- 1 **show mobility-domain config** on page 254

set mobility-domain mode member seed-ip

On a nonseed UNIVERGE WL Controller, sets the IP address of the seed UNIVERGE WL Controller. This command is used on a member UNIVERGE WL Controller to configure it as a member. If the UNIVERGE WL Controller is currently part of another Mobility Domain or using another seed, this command overwrites that configuration.

Syntax **set mobility-domain mode member seed-ip** *ip-addr* [**key** *hex-bytes*]

<i>ip-addr</i>	IP address of the Mobility Domain member, in dotted decimal notation.
key <i>hex-bytes</i>	Fingerprint of the public key to use for UNIVERGE WL Controller-UNIVERGE WL Controller security. Specify the key as 16 hexadecimal bytes. Use a colon between each byte, as in the following example: 00:11:22:33:44:55:66:77:88:99:aa:bb:cc:dd:ee:ff

Defaults None.

Access Enabled.

Examples The following command sets the current UNIVERGE WL Controller as a nonseed member of the Mobility Domain whose seed has the IP address 192.168.1.8:

```
PROMPT# set mobility-domain mode member seed-ip 192.168.1.8
```

```
mode is: member  
seed IP is: 192.168.1.8
```

See Also

- 1 **clear mobility-domain** on page 250
- 1 **show mobility-domain config** on page 254

set mobility-domain mode seed domain-name

Creates a Mobility Domain by setting the current UNIVERGE WL Controller as the seed device and naming the Mobility Domain.

Syntax **set mobility-domain mode seed domain-name** *mob-domain-name*

mob-domain-name Name of the Mobility Domain. Specify between 1 and 32 characters with no spaces.

Defaults None.

Access Enabled.

Usage Before you use this command, the current UNIVERGE WL Controller must have an IP address set with the **set system ip-address** command. After you enter this command, all Mobility Domain traffic is sent and received from the specified IP address.

You must explicitly configure *only one* UNIVERGE WL Controller per domain as the seed. All other UNIVERGE WL Controllers in the domain receive their Mobility Domain information from the seed.

Examples The following command creates a Mobility Domain named Tokyo with the current UNIVERGE WL Controller as the seed:

```
PROMPT# set mobility-domain mode seed domain-name Tokyo  
mode is: seed  
domain name is: Tokyo
```

See Also

- 1 **clear mobility-domain member** on page 250

- 1 **show mobility-domain** on page 254

show mobility-domain config

Displays the configuration of the Mobility Domain.

Syntax **show mobility-domain config**

Defaults None.

Access Enabled.

Examples The following command displays the Mobility Domain configuration:

```
PROMPT# show mobility-domain config
This switch is the seed for domain dang-modo.
10.8.107.1 is a member
10.10.10.66 is a member
```

See Also

- 1 **clear mobility-domain** on page 250
- 1 **set mobility-domain member** on page 251
- 1 **show mobility-domain** on page 254

show mobility-domain

On the seed UNIVERGE WL Controller, displays the Mobility Domain status and members.

Syntax **show mobility-domain**

Defaults None.

Access Enabled.

Examples To display Mobility Domain status, type the following command:

```
PROMPT# show mobility-domain
Mobility Domain name: Tokyo (security required)
Member          State          Type (*:active)  Model          Version
-----
10.8.107.1      STATE_UP        SEED*           WL5100         6.0.1.0
10.10.10.66     STATE_DOWN     MEMBER          WL5100         6.0.1.0
```

Table 28 describes the fields in the display.

Table 28. show mobility-domain Output

Field	Description
Mobility Domain name	Name of the Mobility Domain
Member	IP addresses of the seed UNIVERGE WL Controller and members in the Mobility Domain
State	State of the UNIVERGE WL Controller in the Mobility Domain: <ul style="list-style-type: none"> STATE_UP STATE_DOWN
Status	Role of the UNIVERGE WL Controller in the Mobility Domain: <ul style="list-style-type: none"> MEMBER SEED

See Also

- 1 **clear mobility-domain** on page 250
- 1 **set mobility-domain member** on page 251
- 1 **set mobility-domain mode member seed-ip** on page 252

show mobility-domain
Chapter 10

Network Domain Commands

Use Network Domain commands to configure and manage Network Domain groups.

A Network Domain is a group of geographically dispersed Mobility Domains that share information over a WAN link. This shared information allows a user configured on a UNIVERGE WL Controller in one Mobility Domain to establish connectivity with a UNIVERGE WL Controller in another Mobility Domain in the same Network Domain. The UNIVERGE WL Controller forwards the user traffic by creating a VLAN tunnel to a UNIVERGE WL Controller in the remote Mobility Domain.

In a Network Domain, one or more UNIVERGE WL Controllers serve as a seed UNIVERGE WL Controller. At least one of the Network Domain seeds maintains a connection with each of the member UNIVERGE WL Controllers in the Network Domain. The Network Domain seeds share information about the VLANs configured on their members, so that all the Network Domain seeds have a common database of VLAN information.

This chapter presents Network Domain commands alphabetically. Use the following table to locate commands in this chapter based on their use.

Network Domain	set network-domain mode seed domain-name on page 263
	set network-domain mode member seed-ip on page 261
	set network-domain peer on page 262
	show network-domain on page 263
	clear network-domain on page 258
	clear network-domain mode on page 258
	clear network-domain peer on page 259
	clear network-domain seed-ip on page 260

clear network-domain

Clears all Network Domain configuration and information from a UNIVERGE WL Controller, regardless of whether the UNIVERGE WL Controller is a seed or a member of a Network Domain.

Syntax `clear network-domain`

Defaults None.

Access Enabled.

Usage This command has no effect if the UNIVERGE WL Controller is not configured as part of a Network Domain.

Examples To clear a Network Domain from a UNIVERGE WL Controller within the domain, type the following command:

```
Controller# clear network-domain
This will clear all network-domain configuration. Would you like to continue?
(y/n) [n] y
success: change accepted.
```

See Also

- 1 **set network-domain mode member seed-ip** on page 261
- 1 **set network-domain peer** on page 262
- 1 **set network-domain mode seed domain-name** on page 263

clear network-domain mode

Removes the Network Domain seed or member configuration from the UNIVERGE WL Controller.

Syntax `clear network-domain mode {seed | member}`

seed	Clears the Network Domain seed configuration from the UNIVERGE WL Controller.
member	Clears the Network Domain member configuration from the UNIVERGE WL Controller.

Defaults None.

Access Enabled.

Usage This command has no effect if the UNIVERGE WL Controller is not configured as part of a Network Domain.

Examples The following command clears the Network Domain member configuration from the UNIVERGE WL Controller:

```
Controller# clear network-domain mode member
success: change accepted.
```

The following command clears the Network Domain seed configuration from the UNIVERGE WL Controller:

```
Controller# clear network-domain mode seed
success: change accepted.
```

See Also

- 1 **set network-domain mode member seed-ip** on page 261
- 1 **set network-domain mode seed domain-name** on page 263

clear network-domain peer

Removes the configuration of a Network Domain peer from a UNIVERGE WL Controller configured as a Network Domain seed.

Syntax **clear network-domain peer** {*ip-addr* | **all**}

<i>ip-addr</i>	IP address of the Network Domain peer in dotted decimal notation.
all	Clears the Network Domain peer configuration for all peers from the UNIVERGE WL Controller.

Defaults None.

Access Enabled.

Usage This command has no effect if the UNIVERGE WL Controller is not configured as a Network Domain seed.

clear network-domain seed-ip

Chapter 11

Examples The following command clears the Network Domain peer configuration for peer 192.168.9.254 from the UNIVERGE WL Controller:

```
Controller# clear network-domain peer 192.168.9.254
success: change accepted.
```

The following command clears the Network Domain peer configuration for all peers from the UNIVERGE WL Controller:

```
Controller# clear network-domain peer all
success: change accepted.
```

See Also **set network-domain peer** on page 262

clear network-domain seed-ip

Removes the specified Network Domain seed from the UNIVERGE WL Controller configuration. When you enter this command, the Network Domain TCP connections between the UNIVERGE WL Controller and the specified Network Domain seed are closed.

Syntax **clear network-domain seed-ip** *ip-addr*

ip-addr IP address of the Network Domain seed in dotted decimal notation.

Defaults None.

Access Enabled.

Usage This command has no effect if the UNIVERGE WL Controller is not configured as part of a Network Domain, or if the UNIVERGE WL Controller is not configured as a member of a Network Domain using the specified Network Domain seed.

Examples The following command removes the Network Domain seed with IP address 192.168.9.254 from the UNIVERGE WL Controller configuration:

```
Controller# clear network-domain seed-ip 192.168.9.254
success: change accepted.
```

See Also **set network-domain mode member seed-ip** on page 261

set network-domain mode member seed-ip

Sets the IP address of a Network Domain seed. This command is used for configuring a UNIVERGE WL Controller as a member of a Network Domain. You can specify multiple Network Domain seeds and configure one as the primary seed.

Syntax `set network-domain mode member seed-ip ip-addr [affinity num]`

<i>ip-addr</i>	IP address of the Network Domain seed, in dotted decimal notation.
<i>num</i>	Preference for using the specified Network Domain seed. You can specify a value from 1 through 10. A higher number indicates a greater preference.

Defaults The default affinity for a Network Domain seed is 5.

Access Enabled.

Usage You can specify multiple Network Domain seeds on the UNIVERGE WL Controller. When the UNIVERGE WL Controller needs to connect to a Network Domain seed, it first attempts to connect to the seed with the highest affinity. If that seed is unavailable, the UNIVERGE WL Controller attempts to connect to the seed with the next-highest affinity. After a connection is made to a non-highest-affinity seed, the UNIVERGE WL Controller then periodically attempts to connect to the highest-affinity seed.

Examples The following command sets the UNIVERGE WL Controller as a member of the Network Domain whose seed has the IP address 192.168.1.8:

```
PROMPT# set network-domain mode member seed-ip 192.168.1.8
success: change accepted.
```

The following command sets the UNIVERGE WL Controller as a member of a Network Domain whose seed has the IP address 192.168.9.254 and sets the affinity for that seed to 7. If the UNIVERGE WL Controller specifies other Network Domain seeds, and they are configured with the default affinity of 5, then 192.168.9.254 becomes the primary Network Domain seed for the UNIVERGE WL Controller.

```
PROMPT# set network-domain mode member seed-ip 192.168.9.254 affinity 7
```

set network-domain peer

Chapter 11

success: change accepted.

See Also

- 1 **clear network-domain** on page 258
- 1 **show network-domain** on page 263

set network-domain peer

On a Network Domain seed, configures one or more UNIVERGE WL Controllers as redundant Network Domain seeds. The seeds in a Network Domain share information about the VLANs configured on the member devices, so that all the Network Domain seeds have the same database of VLAN information.

Syntax **set network-domain peer** *ip-addr*

ip-addr IP address of the Network Domain seed to specify as a peer, in dotted decimal notation.

Defaults None.

Access Enabled.

Usage This command must be entered on a UNIVERGE WL Controller configured as a Network Domain seed.

Examples The following command sets the UNIVERGE WL Controller with IP address 192.168.9.254 as a peer of this Network Domain seed:

```
PROMPT# set network-domain peer 192.168.9.254
success: change accepted.
```

See Also

- 1 **clear network-domain** on page 258
- 1 **show network-domain** on page 263

set network-domain mode seed domain-name

Creates a Network Domain by setting the current UNIVERGE WL Controller as a seed device and naming the Network Domain.

Syntax `set network-domain mode seed domain-name net-domain-name`

net-domain-name Name of the Network Domain. Specify between 1 and 16 characters with no spaces.

Defaults None.

Access Enabled.

Usage Before you use this command, the current UNIVERGE WL Controller must have its IP address set with the **set system ip-address** command. After you enter this command, Network Domain traffic is sent and received from the specified IP address.

You can configure multiple UNIVERGE WL Controllers as Network Domain seeds. If you do this, you must identify them as peers by using the **set network domain peer** command.

Examples The following command creates a Network Domain named California with the current UNIVERGE WL Controller as a seed:

```
PROMPT# set network-domain mode seed domain-name California
success: change accepted.
```

See Also

- 1 **clear network-domain** on page 258
- 1 **show network-domain** on page 263

show network-domain

Displays the status of Network Domain seeds and members.

show network-domain

Chapter 11

Syntax `show network-domain`

Defaults None.

Access Enabled.

Examples The output of the command differs based on whether the UNIVERGE WL Controller is a member of a Network Domain or a Network Domain seed. To display Network Domain status, type the following command:

```
PROMPT# show network-domain
```

On a UNIVERGE WL Controller that is a Network Domain member, the following output is displayed:

```
PROMPT# show network-domain
Member Network Domain name: California
Member      State      Mode      Mobility-Domain
-----
10.8.107.1   UP        SEED      default
```

On a UNIVERGE WL Controller that is a Network Domain seed, information is displayed about the Network Domains that UNIVERGE WL Controller is a member, as well as Network Domain seeds with that the UNIVERGE WL Controller has a peer relationship. For example:

```
PROMPT# show network-domain
Network Domain name: California
Peer      State
-----
10.8.107.1   UP
Member      State      Mode      Mobility-Domain
-----
10.1.0.0     DOWN      SEED
Member Network Domain name:
Member      State      Mode      Mobility-Domain
-----
10.8.107.1   UP        MEMBER    default
10.1.0.0     DOWN      SEED
```

Table 29 describes the fields in the display.

Table 29. show network-domain Output

Field	Description
Output if UNIVERGE WL Controller is the Network Domain seed:	
Network Domain name	Name of the Network Domain for which the UNIVERGE WL Controller is a seed.
Peer	IP addresses of the other seeds in the Network Domain.
State	State of the connection between the UNIVERGE WL Controller and the peer Network Domain seeds: <ul style="list-style-type: none"> • UP • DOWN
Member	IP addresses of the seed UNIVERGE WL Controller and members in the Network Domain
State	State of the UNIVERGE WL Controller in the Network Domain: <ul style="list-style-type: none"> • UP • DOWN
Mode	Role of the UNIVERGE WL Controller in the Network Domain: <ul style="list-style-type: none"> • MEMBER • SEED
Mobility-Domain	Name of the Mobility Domain of which the UNIVERGE WL Controller is a member.
Output if UNIVERGE WL Controller is a Network Domain member:	
Member Network Domain name	Name of the Network Domain of which the UNIVERGE WL Controller is a member.
Member	IP addresses of the seed UNIVERGE WL Controller and members in the Network Domain
State	State of the UNIVERGE WL Controller in the Network Domain: <ul style="list-style-type: none"> • UP • DOWN

Table 29. show network-domain Output

Mode	Role of the UNIVERGE WL Controller in the Network Domain: <ul style="list-style-type: none">• MEMBER• SEED
Mobility-Domain	Name of the Mobility Domain of which the UNIVERGE WL Controller is a member.

See Also

- 1 **clear network-domain** on page 258
- 1 **set network-domain mode member seed-ip** on page 261
- 1 **set network-domain mode seed domain-name** on page 263
- 1 **set network-domain peer** on page 262

AP Commands

Use AP commands to configure and manage AP. Be sure to do the following before using the commands:

- 1 Define the country-specific IEEE 802.11 regulations on the UNIVERGE WL Controller. (See **set system countrycode** on page 33.)
- 1 Install the AP and connect it to a port on the UNIVERGE WL Controller.
- 1 Configure an AP. (See **set ap** on page 54.)



Caution! Changing the system country code after AP configuration disables AP and deletes their configuration. If you change the country code on a UNIVERGE WL Controller, you must reconfigure all AP.

This chapter presents AP commands alphabetically. Use the following table to locate commands in this chapter based on their use.

Automatic Configuration of UNIVERGE WL Access Points

set ap auto on page 277

set ap auto mode on page 279

set ap auto radiotype on page 281

set ap auto persistent on page 280

set ap bias on page 282

set ap blink on page 283

set ap radio auto-tune max-power on page 292

set ap radio mode on page 295

	set ap radio radio-profile on page 296
	set ap auto radiotype on page 281
	set ap upgrade-firmware on page 300
External Antenna	set ap radio antennatype on page 291
UNIVERGE WL Access Points-UNIVERGE WL Controller security	set ap fingerprint on page 288
	set ap security on page 298
Static IP Address Assignment for UNIVERGE WL Access Points	set ap boot-configuration ip on page 284
	set ap boot-configuration switch on page 285
	set ap boot-configuration vlan on page 287
	clear ap boot-configuration on page 273
	show ap boot-configuration on page 401
Radio Profile Assignment	set ap radio radio-profile on page 296
	set radio-profile mode on page 316
	clear radio-profile on page 275
	set radio-profile service-profile on page 324
	show radio-profile on page 408
SSID Assignment	set service-profile ssid-name on page 359
	set service-profile ssid-type on page 359
	set service-profile beacon on page 340
Radio Properties	set radio-profile active-scan on page 300
	set radio-profile beacon-interval on page 307
	set radio-profile countermeasures on page 307
	set radio-profile dtim-interval on page 309
	set radio-profile frag-threshold on page 310
	set radio-profile max-rx-lifetime on page 311
	set radio-profile max-tx-lifetime on page 312
	set radio-profile preamble-length on page 320

**Authentication and
Encryption**

set radio-profile rts-threshold on page 323
set service-profile attr on page 334
set service-profile auth-dot1x on page 336
set service-profile auth-fallthru on page 337
set service-profile web-portal-form on page 366
set service-profile auth-psk on page 339
set service-profile wpa-ie on page 372
set service-profile rsn-ie on page 356
set service-profile cipher-ccmp on page 343
set service-profile cipher-tkip on page 343
set service-profile cipher-wep104 on page 344
set service-profile cipher-wep40 on page 346
set service-profile psk-phrase on page 354
set service-profile psk-raw on page 355
set service-profile tkip-mc-time on page 361
set service-profile wep active-multicast-index on page 369
set service-profile wep active-unicast-index on page 370
set service-profile wep key-index on page 371
set service-profile keep-initial-vlan on page 350
set service-profile transmit-rates on page 362
set service-profile long-retry-count on page 351
set service-profile short-retry-count on page 358
set service-profile shared-key-auth on page 357
show service-profile on page 413
clear service-profile on page 276

QoS and VoIP

set radio-profile qos-mode on page 321
set radio-profile max-voip-bw on page 313
set radio-profile max-voip-sessions on page 315

	set service-profile cac-mode on page 341
	set service-profile cac-session on page 342
	set service-profile static-cos on page 360
	set service-profile cos on page 347
	show voip summary on page 424
	show voip max-sessions on page 423
DHCP Restrict	set service-profile dhcp-restrict on page 348
Broadcast control	set service-profile no-broadcast on page 351
Proxy ARP	set service-profile proxy-arp on page 353
Keepalives and session timers	set service-profile active-call-idle-timeout on page 333
	set service-profile idle-client-probing on page 349
	set service-profile user-idle-timeout on page 365
	set service-profile web-portal-session-timeout on page 368
	set service-profile ssid-name on page 359
Radio transmit rates	set service-profile transmit-rates on page 362
	set radio-profile rate-enforcement on page 322
Transmission retries	set service-profile long-retry-count on page 351
	set service-profile short-retry-count on page 358
RF Auto-Tuning	set radio-profile auto-tune channel-config on page 301
	set radio-profile auto-tune channel-holddown on page 303
	set radio-profile auto-tune channel-interval on page 304
	set radio-profile auto-tune power-config on page 305
	set radio-profile auto-tune power-interval on page 306
	set ap radio auto-tune max-power on page 292

	show auto-tune neighbors on page 399
	show auto-tune attributes on page 397
Radio State	set ap radio mode on page 295
Dual Homing	set ap bias on page 282
AP Administration and Maintenance	set ap name on page 290
	set ap blink on page 283
	set ap upgrade-firmware on page 300
	set ap force-image-download on page 289
	reset ap on page 277
	set ap radio channel on page 293
	set ap radio tx-power on page 297
	clear ap radio on page 271
	show ap config on page 374
	show ap group on page 389
	show ap counters on page 378
	show ap global on page 405
	show ap connection on page 403
	show ap unconfigured on page 407
	show ap qos-stats on page 385
	show ap etherstats on page 386
AP Local Switching	show ap arp on page 373
	show ap fdb on page 385
	show ap vlan on page 397

clear ap radio

Disables an AP radio and resets it to its factory default settings.

Syntax clear ap *ap-number* radio {1 | 2 | all}

ap <i>ap-number</i>	Index value that identifies the UNIVERGE WL Access Points on the UNIVERGE WL Controller.
radio 1	Radio 1 of the UNIVERGE WL Access Points.
radio 2	Radio 2 of the UNIVERGE WL Access Points. (This option does not apply to single-radio models.)
radio all	All radios on the AP.

Defaults The **clear ap radio** command resets the radio to the default settings listed in Table 30 and in Table 33 on page 317.

Table 30. Radio-Specific Parameters

Parameter	Default Value	Description
antenna-location	indoors	Location of the radio antenna. Note: This parameter applies only to UNIVERGE WL Access Points models that support external antennas.
antennatype	For most UNIVERGE WL Access Points models, the default is internal .	UNIVERGE WL Control System external antenna model Note: This parameter applies only to UNIVERGE WL Access Points models that support external antennas.
auto-tune max-power	Highest setting allowed for the country of operation or highest setting supported on the hardware, whichever is lower	Maximum percentage of client retransmissions a radio can experience before RF Auto-Tuning considers changing the channel on the radio.
channel	<ul style="list-style-type: none"> 802.11b/g—6 802.11a—Lowest valid channel number for the country of operation 	Number of the channel in which a radio transmits and receives traffic

Table 30. Radio-Specific Parameters

Parameter	Default Value	Description
mode	disable	Operational state of the radio.
radio-profile	None. You must add the radios to a radio profile.	802.11 settings
tx-power	Highest setting allowed for the country of operation or highest setting supported on the hardware, whichever is lower.	Transmit power of a radio, in decibels referred to 1 milliwatt (dBm)

Access Enabled

Usage When you clear a radio, UNIVERGE WL Control System performs the following actions:

- 1 Clears the transmit power, channel, and external antenna setting from the radio.
- 1 Removes the radio from its radio profile and places the radio in the *default* radio profile.

Examples The following command disables and resets radio 2 on the AP 3:

```
PROPMT# clear ap 3 radio 2
```

See Also

- 1 **set ap radio mode** on page 295
- 1 **set ap radio radio-profile** on page 296

clear ap boot-configuration

Removes the static IP address configuration for a UNIVERGE WL Access Points.

Syntax **clear ap boot-configuration** *ap-number*

ap *ap-number* Index value that identifies the UNIVERGE WL Access Points on the UNIVERGE WL Controller.

clear ap boot-configuration

Chapter 12

Defaults None.

Access Enabled.

Usage When the static IP configuration is cleared for a UNIVERGE WL Access Points, and on the UNIVERGE WL Access Points is rebooted, it uses the standard boot process.

Examples The following command clears the static IP address configuration for UNIVERGE WL Access Points 1.

```
PROPMT# clear ap 1 boot-configuration
```

```
This will clear specified AP devices. Would you like to continue? (y/n) [n]y  
success: change accepted.
```

See Also

- 1 **set ap boot-configuration ip** on page 284
- 1 **set ap boot-configuration switch** on page 285
- 1 **set ap boot-configuration vlan** on page 287
- 1 **show ap boot-configuration** on page 401

clear radio-profile

Removes a radio profile or resets one of the profile's parameters to its default value.

Syntax `clear radio-profile name [parameter]`

name Radio profile name.

parameter Radio profile parameter:

- **beacon-interval**
- **countermeasures**
- **dtim-interval**
- **frag-threshold**
- **max-rx-lifetime**
- **max-tx-lifetime**
- **preamble-length**
- **rts-threshold**
- **service-profile**

(For information about these parameters, see the **set radio-profile** commands that use them.)

Defaults If you reset an individual parameter, the parameter is returned to the default value listed in Table 33 on page 317.

Access Enabled.

Usage If you specify a parameter, the setting is reset to its default value. The settings of the other parameters are unchanged and the radio profile remains in the configuration. If you do not specify a parameter, the entire radio profile is deleted from the configuration. All radios that use this profile must be disabled before you can delete the profile.

Examples The following commands disable the radios using radio profile *rp1* and reset the **beaconed-interval** parameter to its default value:

```
PROPMT# set radio-profile rp1 mode disable
PROPMT# clear radio-profile rp1 beacon-interval
success: change accepted.
```

clear service-profile

Chapter 12

The following commands disable the radios using radio profile *rp6* and remove the profile:

```
PROPMT# set radio-profile rp6 mode disable
PROPMT# clear radio-profile rp6
success: change accepted.
```

See Also

- 1 **set ap radio radio-profile** on page 296
- 1 **set radio-profile mode** on page 316
- 1 **show ap config** on page 374
- 1 **show radio-profile** on page 408

clear service-profile

Removes a service profile or resets one of the profile's parameters to its default value.

Syntax **clear service-profile** *name*

name Service profile name.

Defaults None.

Access Enabled.

Usage If the service profile is mapped to a radio profile, you must remove it from the radio profile first. (After disabling all radios that use the radio profile, use the **clear radio-profile** *name* **service-profile** *name* command.)

Examples The following commands disable the radios using radio profile *rp6*, remove service-profile *svcprof6* from *rp6*, then clear *svcprof6* from the configuration.

```
PROPMT# set radio-profile rp6 mode disable
PROPMT# clear radio-profile rp6 service-profile svcprof6
success: change accepted.
PROPMT# clear service-profile svcprof6
success: change accepted.
```

- 1 **clear radio-profile** on page 275
- 1 **set radio-profile mode** on page 316
- 1 **show service-profile** on page 413

reset ap

Restarts an AP.

Syntax `reset ap ap-number`

ap *ap-number* Index value that identifies the UNIVERGE WL Access Points on the UNIVERGE WL Controller.

Defaults None.

Access Enabled.

Usage When you enter this command, the AP drops all sessions and reboots.



Caution! Restarting an AP can cause data loss for users who are currently associated with the AP.

Examples The following command resets AP 7:

```
PROPMT# reset ap 7
This will reset specified AP devices. Would you like to continue? (y/n)y
success: rebooting ap 7
```

set ap auto

Creates a profile for automatic configuration of UNIVERGE WL Access Points.

Syntax `set ap auto`

Defaults None.

Access Enabled.

Usage Table 31 lists the configurable profile parameters and their defaults. The only parameter that requires configuration is the profile mode. The profile is disabled by default. To use the profile to configure UNIVERGE WL Access Points, you must enable the profile using the **set ap auto mode enable** command.

The profile uses the *default* radio profile by default. You can change the profile using the **set ap auto radio radio-profile** command. You can use set ap auto commands to change settings for the parameters listed in Table 31. (The commands are listed in the “See Also” section.)

Table 31. Configurable Profile Parameters for UNIVERGE WL Access Points

Parameter	Default Value
UNIVERGE WL Access Points Parameters	
bias	high
blink	disable
(Not shown in show ap config output)	
force-image-download	disable (NO)
group (load balancing group)	none
mode	disabled
persistent	none
upgrade-firmware (boot-download-enable)	enable (YES)
Radio Parameters	
radio <i>num</i> auto-tune max-power	default
radio <i>num</i> mode	enabled
radio <i>num</i> radio-profile	default
radiotype	11g (or 11b for country codes where 802.11g is not allowed)

Examples The following command creates a profile for automatic UNIVERGE WL Access Points configuration:

```
PROPMT# set ap auto
success: change accepted.
```

See Also

- 1 **set ap auto mode** on page 279
- 1 **set ap auto persistent** on page 280
- 1 **set ap auto radiotype** on page 281
- 1 **set ap bias** on page 282
- 1 **set ap blink** on page 283
- 1 **set ap radio auto-tune max-power** on page 292
- 1 **set ap radio mode** on page 295
- 1 **set ap radio radio-profile** on page 296
- 1 **set ap upgrade-firmware** on page 300

set ap auto mode

Enables a UNIVERGE WL Controller profile for automatic UNIVERGE WL Access Points configuration.

Syntax **set ap auto mode {enable | disable}**

enable Enables the UNIVERGE WL Access Points configuration profile.

disable Disables the UNIVERGE WL Access Points configuration profile.

Defaults The UNIVERGE WL Access Points configuration profile is disabled by default.

Access Enabled.

set ap auto persistent

Chapter 12

Usage You must use the **set ap auto** command to create the profile before you can enable it.

Examples The following command enables the profile for automatic UNIVERGE WL Access Points configuration:

```
PROPMT# set ap auto mode enable
success: change accepted.
```

See Also

- 1 **set ap auto** on page 277
- 1 **set ap auto persistent** on page 280
- 1 **set ap auto radiotype** on page 281
- 1 **set ap bias** on page 282
- 1 **set ap blink** on page 283
- 1 **set ap radio auto-tune max-power** on page 292
- 1 **set ap radio mode** on page 295
- 1 **set ap radio radio-profile** on page 296
- 1 **set ap upgrade-firmware** on page 300

set ap auto persistent

Converts a temporary UNIVERGE WL Access Points configuration created by the UNIVERGE WL Access Points configuration profile into a persistent UNIVERGE WL Access Points configuration on the UNIVERGE WL Controller.

Syntax **set ap auto persistent** [*ap-number* | **all**]

<i>ap-number</i>	Index value that identifies the UNIVERGE WL Access Points on the UNIVERGE WL Controller.
all	Converts the configurations of all Auto-APs being managed by the UNIVERGE WL Controller into permanent configurations.

Defaults None.

Access Enabled.

Usage To display the UNIVERGE WL Access Points numbers assigned to Auto-APs, use the **show ap status all** command.

Examples The following command converts the configuration of Auto-AP 5 into a permanent configuration:

```
PROPMT# set ap auto persistent 5
success: change accepted.
```

See Also

- 1 **set ap auto** on page 277
- 1 **set ap auto mode** on page 279
- 1 **set ap auto radiotype** on page 281

set ap auto radiotype

Sets the radio type for single-UNIVERGE WL Access Points radios that use the UNIVERGE WL Access Points configuration profile.

Syntax **set ap auto [radiotype { 11a | 11b | 11g }]**

radiotype 11a | 11b | 11g

Radio type:

- **11a**—802.11a
- **11b**—802.11b
- **11g**—802.11g

Defaults The default radio type for models WL1500-AP, WL1500-AP-JP and WL1700-MS(AP) and for the 802.11b/g radios, or 802.11b in regulatory domains that do not support 802.11g.

Access Enabled.

Examples The following command sets the radio type to 802.11b:

```
PROPMT# set ap auto radiotype 11b
success: change accepted.
```

See Also

- 1 **set ap auto** on page 277
- 1 **set ap auto mode** on page 279
- 1 **set ap auto persistent** on page 280

set ap bias

Changes the bias for a UNIVERGE WL Access Point. Bias is the priority of one UNIVERGE WL Controller over other UNIVERGE WL Controllers for booting and configuring the UNIVERGE WL Access Points.

Syntax **set ap** {*ap-number* | **auto**} **bias** {**high** | **low**}

ap <i>ap-number</i>	Index value that identifies the UNIVERGE WL Access Points on the UNIVERGE WL Controller.
ap auto	Configures bias for the UNIVERGE WL Access Points configuration profile. (See set ap auto on page 277.)
high	High bias.
low	Low bias.

Defaults The default bias is high.

Access Enabled.

Usage High bias is preferred over low bias. Bias applies only to UNIVERGE WL Controllers indirectly attached to the UNIVERGE WL Access Points through an intermediate Layer 2 or Layer 3 network. A UNIVERGE WL Access Point always attempts to boot on UNIVERGE WL Access Points port 1 first, and if a UNIVERGE WL Controller is directly attached on UNIVERGE WL Access Points port 1, the UNIVERGE WL Access Points always boots from it.

If UNIVERGE WL Access Points port 1 is indirectly connected to UNIVERGE WL Controllers through the network, the UNIVERGE WL Access Points boots from the UNIVERGE WL Controller with the high bias for the UNIVERGE WL Access Points. If the bias for all connections is the same, the UNIVERGE WL Access Points selects the UNIVERGE WL Controller that has the greatest capacity to add more active UNIVERGE WL Access Points. For example, if a UNIVERGE WL Access Point is dual homed to two UNIVERGE WL Controllers,

and one of the UNIVERGE WL Controllers has 3 active UNIVERGE WL Access Points while the other UNIVERGE WL Controller has 2 active UNIVERGE WL Access Points, the new UNIVERGE WL Access Points selects the UNIVERGE WL Controller that has only 2 active UNIVERGE WL Access Points.

If the boot request on UNIVERGE WL Access Points port 1 fails, the UNIVERGE WL Access Points attempts to boot over its port 2, using the same process described above.

UNIVERGE WL Access Points selection of a UNIVERGE WL Controller is *sticky*. After a UNIVERGE WL Access Point selects a UNIVERGE WL Controller to boot from, the UNIVERGE WL Access Points continues to use that UNIVERGE WL Controller for its active data link even if another UNIVERGE WL Controller configured with high bias for the UNIVERGE WL Access Points becomes available.

The following command changes the bias for an AP to low:

```
PROPMT# set ap 1 bias low
success: change accepted.
```

See Also `show ap config` on page 374

set ap blink

Enables or disables LED blink mode on an AP to make it easy to identify. When blink mode is enabled on WL-xxx models, the health and radio LEDs alternately blink green and amber. When blink mode is enabled on an WL1500-AP, the 11a LED blinks on and off. By default, blink mode is disabled.

Syntax `set ap {ap-number | auto} blink {enable | disable}`

ap ap-number	Index value that identifies the UNIVERGE WL Access Points on the UNIVERGE WL Controller.
ap auto	Configures blink mode for the UNIVERGE WL Access Points configuration profile. (See <code>set ap auto</code> on page 277.)
enable	Enables blink mode.
disable	Disables blink mode.

set ap boot-configuration ip

Chapter 12

Defaults LED blink mode is disabled by default.

Access Enabled.

Usage Changing the LED blink mode does not alter operation of the AP. Only the behavior of the LEDs is affected.

Examples The following command enables LED blink mode on the AP 3 and 4:

```
PROPMT# set ap 3-4 blink enable
success: change accepted.
```

set ap boot-configuration ip

Specifies static IP address information for a UNIVERGE WL Access Points.

Syntax **set ap** *ap-number* **boot-configuration ip** *ip-addr* **netmask** *mask-addr* **gateway** *gateway-addr* [**mode** {**enable** | **disable**}]

ap <i>ap-number</i>	Index value that identifies the UNIVERGE WL Access Points on the UNIVERGE WL Controller.
ip <i>ip-addr</i>	The IP address to be assigned to the UNIVERGE WL Access Points, in dotted decimal notation (for example, 10.10.10.10).
netmask <i>mask-addr</i>	The subnet mask, in dotted decimal notation (for example, 255.255.255.0).
gateway <i>gateway-addr</i>	The IP address of the next-hop router, in dotted decimal notation.
mode { enable disable }	Enables or disables the static IP address for the UNIVERGE WL Access Points.

Defaults By default UNIVERGE WL Access Points use DHCP to obtain an IP address, rather than a using a manually assigned IP address.

Access Enabled.

Usage Normally, UNIVERGE WL Access Points use DHCP to obtain IP address information. In some installations, DHCP may not be available. In this case, you can assign static IP address information to the UNIVERGE WL Access Points, including the UNIVERGE WL Access Point IP address and netmask, and default gateway.

If the manually assigned IP information is incorrect, the UNIVERGE WL Access Points uses DHCP to obtain its IP address.

Examples The following command configures UNIVERGE WL Access Points 1 to use IP address 172.16.0.42 with a 24-bit netmask, and use 172.16.0.20 as its default gateway:

```
PROPMT# set ap 1 boot-configuration ip 172.16.0.42 netmask 255.255.255.0 gateway
172.16.0.20
success: change accepted.
```

See Also

- 1 **clear ap boot-configuration** on page 273
- 1 **set ap boot-configuration switch** on page 285
- 1 **set ap boot-configuration vlan** on page 287
- 1 **show ap boot-configuration** on page 401

set ap boot-configuration switch

Specifies the UNIVERGE WL Controller that a UNIVERGE WL Access Points contacts and attempts to use as its boot device.

Syntax **set ap** *ap-number* **boot-configuration switch** [**switch-ip** *ip-addr*] [**name** *name* **dns** *ip-addr*] [**mode** {**enable** | **disable**}]

ap <i>ap-number</i>	Index value that identifies the UNIVERGE WL Access Points on the UNIVERGE WL Controller.
switch-ip <i>ip-addr</i>	The IP address of the UNIVERGE WL Controller the UNIVERGE WL Access Points should boot from.
name <i>name</i>	The fully qualified domain name of the UNIVERGE WL Controller that the UNIVERGE WL Access Points boots from. When both a name and a switch-ip are specified, the UNIVERGE WL Access Points uses the name.

set ap boot-configuration switch

Chapter 12

dns ip-addr	The IP address of the DNS server used to resolve the specified name of the UNIVERGE WL Controller.
mode {enable disable}	Enables or disables the UNIVERGE WL Access Points using the specified boot device.

Defaults By default UNIVERGE WL Access Points use the process described in “Default UNIVERGE WL Access Points Boot Process”, in the *Configuration Guide* to boot from a UNIVERGE WL Controller, instead of using a manually specified UNIVERGE WL Controller.

Access Enabled.

Usage When you specify a boot UNIVERGE WL Controller for a UNIVERGE WL Access Points to boot from, it boots using the process described in “UNIVERGE WL Access Points Boot Process Using Static IP Configuration”, in the *Configuration Guide*.

When a static IP address is specified for a UNIVERGE WL Access Points, there is no preconfigured DNS information or DNS name for the UNIVERGE WL Controller that the UNIVERGE WL Access Points attempts to use as its boot device. If you configure a static IP address for a UNIVERGE WL Access Points, but do not specify a boot device, then the UNIVERGE WL Controller must be reachable via subnet broadcast.

Examples The following command configures UNIVERGE WL Access Points 1 to use a UNIVERGE WL Controller with address 172.16.0.21 as its boot device.

```
PROPMT# set ap 1 boot-configuration switch switch-ip 172.16.0.21 mode enable
success: change accepted.
```

The following command configures UNIVERGE WL Access Points 1 to use the UNIVERGE WL Controller with the name controller2 as its boot device. The DNS server at 172.16.0.1 is used to resolve the name of the UNIVERGE WL Controller.

```
PROPMT# set ap 1 boot-configuration switch name controller2 dns 172.16.0.1 mode
enable
success: change accepted.
```

See Also

- 1 **clear ap boot-configuration** on page 273
- 1 **set ap boot-configuration ip** on page 284
- 1 **set ap boot-configuration vlan** on page 287
- 1 **show ap boot-configuration** on page 401

set ap boot-configuration vlan

Specifies 802.1Q VLAN tagging information for a UNIVERGE WL Access Points.

Syntax `set ap ap-number boot-configuration vlan vlan-tag tag-value [mode {enable | disable}]`

Syntax `set ap ap-number boot-configuration vlan mode {enable | disable}`

ap <i>ap-number</i>	Index value that identifies the UNIVERGE WL Access Points on the UNIVERGE WL Controller.
vlan-tag <i>tag-value</i>	The VLAN tag value. You can specify a number from 1 – 4093.
mode {enable disable}	Enables or disables use of the specified VLAN tag on the UNIVERGE WL Access Points.

Defaults None.

Access Enabled.

Usage When this command is configured, all Ethernet frames emitted from the UNIVERGE WL Access Points are formatted with an 802.1Q tag with a specified VLAN number. Frames sent to the UNIVERGE WL Access Points that are not tagged with this value are ignored.

Examples The following command configures UNIVERGE WL Access Points 1 to use VLAN tag 100:

```
PROPMT# set ap 1 boot-configuration vlan vlan-tag 100 mode enable
success: change accepted.
```

See Also

- 1 **clear ap boot-configuration** on page 273
- 1 **set ap boot-configuration ip** on page 284
- 1 **set ap boot-configuration switch** on page 285
- 1 **show ap boot-configuration** on page 401

set ap fingerprint

Verifies a UNIVERGE WL Access Point fingerprint on a UNIVERGE WL Controller. If UNIVERGE WL Access Points-UNIVERGE WL Controller security is required by a UNIVERGE WL Controller, a UNIVERGE WL Access Point can establish a management session with the UNIVERGE WL Controller only if you have verified the UNIVERGE WL Access Point identity by verifying its fingerprint on the UNIVERGE WL Controller.

Syntax **set ap** *ap-number* **fingerprint** *fingerprint*

ap <i>ap-number</i>	Index value that identifies the UNIVERGE WL Access Points on the UNIVERGE WL Controller.
<i>fingerprint</i>	The 16-digit hexadecimal number of the fingerprint. Use a colon between each digit. Make sure the fingerprint you enter matches the fingerprint used by the UNIVERGE WL Access Points.

Defaults None.

Access Enabled.

Usage UNIVERGE WL Access Points are configured with an encryption key pair at the factory. The fingerprint for the public key is displayed on a label on the back of the UNIVERGE WL Access Points, in the following format:

RSA
aaaa:aaaa:aaaa:aaaa:
aaaa:aaaa:aaaa:aaaa

If a UNIVERGE WL Access Point is already installed and operating, you can use the **show ap status** command to display the fingerprint. The **show ap config** command lists the UNIVERGE WL Access Point fingerprint only if the fingerprint has been verified in UNIVERGE WL Control System. If the fingerprint has not been verified, the fingerprint information in the command output is blank.

Examples The following example verifies the fingerprint for UNIVERGE WL Access Points 8:

```
PROPMT# set ap 8 fingerprint b4:f9:2a:52:37:58:f4:d0:10:75:43:2f:45:c9:52:c3
success: change accepted.
```

See Also

- 1 **set ap security** on page 298
- 1 **show ap config** on page 374
- 1 **show ap group** on page 389

set ap force-image-download

Configures a UNIVERGE WL Access Point to download its software image from the UNIVERGE WL Controller instead of loading the image that is locally stored on the UNIVERGE WL Access Point.

Syntax **set ap auto force-image-download {enable | disable}**

ap auto Configures forced image download for the UNIVERGE WL Access Point configuration profile. (See **set ap auto** on page 277.)

force-image-download enable Enables forced image download.

force-image-download disable Disables forced image download.

Defaults Forced image download is disabled by default.

Access Enabled.

set ap name

Chapter 12

Usage A change to the forced image download option takes place the next time the UNIVERGE WL Access Point is restarted.

Even when forced image download is disabled (the default), the UNIVERGE WL Access Point still checks with the UNIVERGE WL Controller to verify that the UNIVERGE WL Access Point has the latest image.

The UNIVERGE WL Access Point loads its local image only if the UNIVERGE WL Controller does not have a newer UNIVERGE WL Access Point image than the one in the UNIVERGE WL Access Point local storage. If the UNIVERGE WL Controller has a newer version of the UNIVERGE WL Access Point image than the version in the UNIVERGE WL Access Point's local storage, the UNIVERGE WL Access Point loads its image from the UNIVERGE WL Controller.

Examples The following command enables forced image download on UNIVERGE WL Access Points 69:

```
PROPMT# set ap 69 force-image-download enable
success: change accepted.
```

See Also **show ap config** on page 374

set ap name

Changes an AP name.

Syntax **set ap** *ap-number* **name** *name*

ap *ap-number* Index value that identifies the UNIVERGE WL Access Points on the UNIVERGE WL Controller.

name Alphanumeric string of up to 16 characters, with no spaces.

Defaults The default name of a directly attached UNIVERGE WL Access Points is based on the port number of the UNIVERGE WL Access Points access port attached to the UNIVERGE WL Access Points. For example, the default name for a UNIVERGE WL Access Point on UNIVERGE WL Access Points access port 1 is *AP01*.

Access Enabled.

Examples The following command changes the name of the AP 1 to *techpubs*:

```
PROPMT# set ap 1 name techpubs
success: change accepted.
```

See Also `show ap config` on page 374

set ap radio antennatype

Sets the model number for an external antenna.

```
set ap ap-number radio {1 | 2} antennatype {ANT1060 | ANT1120 |
ANT1180 | WL-ANT2060 | WL-ANT2120 | WL-ANT2180 | ANT5060 |
ANT5060 | ANT5120 | ANT5180 | WL-ANT5060 | WL-ANT5120 | WL-ANT5180 |
internal}
```

ap *ap-number*

Index value that identifies the UNIVERGE WL Access Points on the UNIVERGE WL Controller.

radio 1

Radio 1 of the UNIVERGE WL Access Points.

radio 2

Radio 2 of the UNIVERGE WL Access Points. (This option does not apply to single-radio models.)

antennatype

```
{ANT1060 | ANT1120 |
ANT1180 | WL-ANT2060 |
WL-ANT2120 | WL-ANT2180 |
internal}
```

802.11b/g external antenna models:

- ANT1060—60° 802.11b/g antenna
- ANT1120—120° 802.11b/g antenna
- ANT1180—180° 802.11b/g antenna
- WL-ANT2060—60° 802.11b/g antenna
- WL-ANT2120—120° 802.11b/g antenna
- WL-ANT2180—180° 802.11b/g antenna
- internal—Uses the internal antenna instead

set ap radio auto-tune max-power

Chapter 12

antennatype

{ANT5060 | ANT5120 |
ANT5180 | WL-ANT5060 |
WL-ANT5120 | WL-ANT5180 |
internal}

802.11a external antenna models:

- ANT5060—60° 802.11a antenna
- ANT5120—120° 802.11a antenna
- ANT5180—180° 802.11a antenna
- WL-ANT5060—60° 802.11a antenna
- WL-ANT5120—120° 802.11a antenna
- WL-ANT5180—180° 802.11a antenna
- internal—Uses the internal antenna instead

Defaults All radios use the internal antenna by default, if the UNIVERGE WL Access Points model has an internal antenna.

Access Enabled.

Examples The following command configures the 802.11b/g radio on UNIVERGE WL Access Points 1 to use antenna model WL-ANT2060:

```
PROPMT# set ap 1 radio 1 antennatype WL-ANT2060  
success: change accepted.
```

See Also **show ap config** on page 374

set ap radio auto-tune max-power

Sets the maximum power that RF Auto-Tuning can set on a radio.

Syntax **set ap** {*ap-number* | **auto**} **radio** {**1** | **2**} **auto-tune max-power**
power-level

ap *ap-number*

Index value that identifies the UNIVERGE WL Access Points on the UNIVERGE WL Controller.

ap auto

Sets the maximum power for radios configured by the UNIVERGE WL Access Points configuration profile. (See **set ap auto** on page 277.)

radio 1

Radio 1 of the UNIVERGE WL Access Points.

radio 2

Radio 2 of the UNIVERGE WL Access Points.
(This option does not apply to single-radio models.)

power-level

Maximum power setting RF Auto-Tuning can assign to the radio, expressed as the number of decibels in relation to 1 milliwatt (dBm). You can specify a value from 1 up to the maximum value allowed for the country of operation.

The *power-level* can be a value from 1 to 20.

Defaults The default maximum power setting that RF Auto-Tuning can set on a radio is the highest setting allowed for the country of operation or highest setting supported on the hardware, whichever is lower.

Access Enabled.

Examples The following command sets the maximum power that RF Auto-Tuning can set on radio 1 on the UNIVERGE WL Access Points 3 to 12 dBm.

```
PROPMT# set ap 3 radio 1 auto-tune max-power 12
success: change accepted.
```

See Also

- 1 **set radio-profile auto-tune power-config** on page 305
- 1 **set radio-profile auto-tune power-interval** on page 306

set ap radio channel

Sets an AP radio channel.

Syntax **set ap** *ap-number* **radio** {**1** | **2**} **channel** *channel-number*

ap *ap-number*

Index value that identifies the UNIVERGE WL Access Points on the UNIVERGE WL Controller.

radio 1

Radio 1 of the UNIVERGE WL Access Points.

set ap radio channel

Chapter 12

radio 2	Radio 2 of the UNIVERGE WL Access Points. (This option does not apply to single-radio models.)
channel <i>channel-number</i>	Channel number. The valid channel numbers depend on the country of operation.

Defaults The default channel depends on the radio type:

- 1 The default channel number for 802.11b/g is 6.
- 1 The default channel number for 802.11a is the lowest valid channel number for the country of operation.

Access Enabled.

Usage You can configure the transmit power of a radio on the same command line. Use the **tx-power** option.

This command is not valid if dynamic channel tuning (RF Auto-Tuning) is enabled.

Examples The following command configures the channel on the 802.11a radio on the AP 5:

```
PROPMT# set ap 5 radio 1 channel 36
success: change accepted.
```

The following command configures the channel and transmit power on the 802.11b/g radio on the AP 1:

```
PROPMT# set ap 1 radio 1 channel 1 tx-power 10
success: change accepted.
```

See Also

- 1 **set ap radio tx-power** on page 297
- 1 **show ap config** on page 374

set ap radio mode

Enables or disables a radio on an AP.

Syntax `set ap {ap-number | auto} radio {1 | 2} mode {enable | disable}`

ap <i>ap-number</i>	Index value that identifies the UNIVERGE WL Access Points on the UNIVERGE WL Controller.
ap auto	Sets the radio mode for UNIVERGE WL Access Points managed by the UNIVERGE WL Access Points configuration profile. (See set ap auto on page 277.)
radio 1	Radio 1 of the UNIVERGE WL Access Points.
radio 2	Radio 2 of the UNIVERGE WL Access Points. (This option does not apply to single-radio models.)
mode enable	Enables a radio.
mode disable	Disables a radio.

Defaults AP access point radios are disabled by default.

Access Enabled.

Usage To enable or disable one or more radios to which a profile is assigned, use the **set ap radio radio-profile** command. To enable or disable all radios that use a specific radio profile, use the **set radio-profile** command.

Examples The following command enables radio 1 on the AP 1:

```
PROPMT# set ap 1 radio 1 mode enable
success: change accepted.
```

See Also

- 1 **clear ap radio** on page 271
- 1 **set ap radio radio-profile** on page 296
- 1 **set radio-profile mode** on page 316
- 1 **show ap config** on page 374

set ap radio radio-profile

Assigns a radio profile to an AP radio and enables or disables the radio.

Syntax **set ap** {*ap-number* | **auto**} **radio** {**1** | **2**}
radio-profile *name* **mode** {**enable** | **disable**}

ap <i>ap-number</i>	Index value that identifies the UNIVERGE WL Access Points on the UNIVERGE WL Controller.
ap auto	Sets the radio profile for the UNIVERGE WL Access Points configuration profile. (See set ap auto on page 277.)
radio 1	Radio 1 of the UNIVERGE WL Access Points.
radio 2	Radio 2 of the UNIVERGE WL Access Points. (This option does not apply to single-radio models.)
radio-profile <i>name</i>	Radio profile name of up to 16 alphanumeric characters, with no spaces.
mode enable	Enables radios on the specified ports with the parameter settings in the specified radio profile.
mode disable	Disables radios on the specified ports.

Defaults None.

Access Enabled.

Usage When you create a new profile, the radio parameters in the profile are set to their factory default values.

To enable or disable all radios using a specific radio profile, use **set radio-profile**.

Examples The following command enables radio 1 on AP 1 assigned to radio profile *rp1*:

```
PROPMT# set ap 1 radio 1 radio-profile rp1 mode enable
success: change accepted.
```

See Also

- 1 **clear ap radio** on page 271
- 1 **set ap radio mode** on page 295

- 1 **set radio-profile mode** on page 316
- 1 **show radio-profile** on page 408

set ap radio tx-power

Sets the transmit power of an AP radio.

Syntax **set ap** *ap-number* **radio** {**1** | **2**} **tx-power** *power-level*

ap <i>ap-number</i>	Index value that identifies the UNIVERGE WL Access Points on the UNIVERGE WL Controller.
radio 1	Radio 1 of the UNIVERGE WL Access Points.
radio 2	Radio 2 of the UNIVERGE WL Access Points. (This option does not apply to single-radio models.)
tx-power <i>power-level</i>	Number of decibels in relation to 1 milliwatt (dBm). The valid values depend on the country of operation.

Note: The maximum transmit power you can configure on any NEC Networks radio is the maximum allowed for the country in which you plan to operate the radio *or* one of the following values if that value is less than the country maximum: on an 802.11a radio, 11 dBm for channel numbers less than or equal to 64, or 10 dBm for channel numbers greater than 64; on an 802.11b/g radio, 16 dBm for all valid channel numbers for 802.11b, or 14 dBm for all valid channel numbers for 802.11g.

Defaults The default transmit power on all AP radio types is the highest setting allowed for the country of operation or highest setting supported on the hardware, whichever is lower.

Access Enabled.

Usage You also can configure a radio channel on the same command line. Use the **channel** option.

This command is not valid if dynamic power tuning (RF Auto-Tuning) is enabled.

set ap security

Chapter 12

Examples The following command configures the transmit power on the 802.11a radio on the AP connected 3:

```
PROPMT# set ap 3 radio 1 tx-power 10
success: change accepted.
```

The following command configures the channel and transmit power on the 802.11b/g radio on the AP 1:

```
PROPMT# set ap 1 radio 1 channel 1 tx-power 10
success: change accepted.
```

See Also

- 1 **set ap radio channel** on page 293
- 1 **show ap config** on page 374

set ap security

Sets security requirements for management sessions between a UNIVERGE WL Controller and its UNIVERGE WL Access Points.



Note. The maximum transmission unit (MTU) for encrypted UNIVERGE WL Access Points management traffic is 1498 bytes, whereas the MTU for unencrypted management traffic is 1474 bytes. Make sure the devices in the intermediate network between the UNIVERGE WL Controller and UNIVERGE WL Access Points can support the higher MTU.

Syntax **set ap security** *secsetting* {**require** | **optional** | **none**}

security *secsetting* Name of the security security setting.

require Requires all UNIVERGE WL Access Points to have encryption keys that have been verified in the CLI by an administrator. If a UNIVERGE WL Access Point does not have an encryption key or the key has not been verified, the UNIVERGE WL Controller does not establish a management session with the UNIVERGE WL Access Points.

optional	Allows UNIVERGE WL Access Points to be managed by the UNIVERGE WL Controller even if they do not have encryption keys or their keys have not been verified by an administrator. Encryption is used for UNIVERGE WL Access Points that support it.
none	Encryption is not used, even for UNIVERGE WL Access Points that support it.

Defaults The default setting is **optional**.

Access Enabled.

Usage This parameter applies to all UNIVERGE WL Access Points managed by the UNIVERGE WL Controller. If you change the setting to **required**, the UNIVERGE WL Controller requires UNIVERGE WL Access Points to have encryption keys. The UNIVERGE WL Controller also requires their fingerprints to be verified in UNIVERGE WL Control System. When UNIVERGE WL Access Points security is required, a UNIVERGE WL Access Point can establish a management session with the UNIVERGE WL Controller only if its fingerprint has been verified by you in UNIVERGE WL Control System.

A change to UNIVERGE WL Access Points security support does not affect management sessions that are already established. To apply the new setting to a UNIVERGE WL Access Point, restart the UNIVERGE WL Access Point.

Examples The following command configures a UNIVERGE WL Controller to require UNIVERGE WL Access Points to have encryption keys:

```
PROPMT# set ap security require
```

See Also

- 1 **set ap fingerprint** on page 288
- 1 **show ap config** on page 374
- 1 **show ap group** on page 389

set ap upgrade-firmware

Disables or reenables automatic upgrade of an AP boot firmware.

Syntax `set ap auto upgrade-firmware {enable | disable}`

ap auto	Configures firmware upgrades for the UNIVERGE WL Access Points configuration profile. (See set ap auto on page 277.)
enable	Enables automatic firmware upgrades.
disable	Disables automatic firmware upgrades.

Defaults Automatic firmware upgrades of AP are enabled by default.

Access Enabled.

Usage When the feature is enabled on a UNIVERGE WL Controller port, an AP connected to that port upgrades its boot firmware to the latest version stored on the UNIVERGE WL Controller.

Examples The following command disables automatic firmware upgrades on the AP 3:

```
PROPMT# set ap 3 upgrade-firmware disable
```

See Also `show ap config` on page 374

set radio-profile active-scan

Disables or reenables active RF detection scanning on the UNIVERGE WL Access Points radios managed by a radio profile. When active scanning is enabled, UNIVERGE WL Access Points radios look for rogue devices by sending *probe any* requests (probe requests with a null SSID name), to solicit probe responses from other access points.

Passive scanning is always enabled and cannot be disabled. During passive scanning, radios look for rogues by listening for beacons and probe responses.

Syntax `set radio-profile name active-scan {enable | disable}`

<i>name</i>	Radio profile name.
enable	Configures radios to actively scan for rogues.
disable	Configures radios to scan only passively for rogues by listening for beacons and probe responses.

Defaults Active scanning is enabled by default.

Access Enabled.

Usage You can enter this command on any UNIVERGE WL Controller in the Mobility Domain. The command takes effect only on that UNIVERGE WL Controller.

Examples The following command disables active scan in radio profile *radprof3*:

```
PROPMT# set radio-profile radprof3 active-scan disable
success: change accepted.
```

See Also `show radio-profile` on page 408

set radio-profile auto-tune channel-config

Disables or reenables dynamic channel tuning (RF Auto-Tuning) for the UNIVERGE WL Access Points radios in a radio profile.

Syntax `set radio-profile name auto-tune channel-config {enable | disable} [no-client]`

<i>name</i>	Radio profile name.
enable	Configures radios to dynamically select their channels when the radios are started.
disable	Configures radios to use their statically assigned channels, or the default channels if unassigned, when the radios are started.
no-client	Configures radios to change channels regardless of client status. Without this option, a radio changes the channel only if the radio does not have any active clients on that channel.

set radio-profile auto-tune channel-config

Chapter 12

Defaults Dynamic channel assignment is enabled by default.

Access Enabled.

Usage If you disable RF Auto-Tuning for channels, UNIVERGE WL Control System does not dynamically set the channels when radios are first enabled and also does not tune the channels during operation.

If RF Auto-Tuning for channels is enabled, UNIVERGE WL Control System does not allow you to manually change channels.

Even when RF Auto-Tuning for channels is enabled, UNIVERGE WL Control System does not change the channel on radios that have active client sessions, unless you use the no-client option.

RF Auto-Tuning of channels on 802.11a radios uses only the bottom eight channels in the band (36, 40, 44, 48, 52, 56, 60, and 64). To use a higher channel number, you must disable RF Auto-Tuning of channels on the radio profile the radio is in, and use the **set ap radio channel** command to statically configure the channel.

Examples The following command disables dynamic channel tuning for radios in the *rp2* radio profile:

```
PROPMT# set radio-profile rp2 auto-tune channel-config disable
success: change accepted.
```

See Also

- 1 **set ap radio channel** on page 293
- 1 **set radio-profile auto-tune channel-holddown** on page 303
- 1 **set radio-profile auto-tune channel-interval** on page 304
- 1 **set radio-profile auto-tune power-config** on page 305
- 1 **show radio-profile** on page 408

set radio-profile auto-tune channel-holddown

Sets the minimum number of seconds a radio in a radio profile must remain at its current channel assignment before RF Auto-Tuning can change the channel. The channel holddown provides additional stability to the network by preventing the radio from changing channels too rapidly in response to spurious RF anomalies such as short-duration channel interference.

Syntax `set radio-profile name auto-tune channel-holddown holddown`

<i>name</i>	Radio profile name.
<i>rate</i>	Minimum number of seconds a radio must remain on its current channel setting before RF Auto-Tuning is allowed to change the channel. You can specify from 0 to 65535 seconds.

Defaults The default RF Auto-Tuning channel holddown is 900 seconds.

Access Enabled.

Usage The channel holddown applies even if RF anomalies occur that normally cause an immediate channel change.

Examples The following command changes the channel holddown for radios in radio profile *rp2* to 600 seconds:

```
PROPMT# set radio-profile rp2 auto-tune channel-holddown 600
success: change accepted.
```

See Also

- 1 **set radio-profile auto-tune channel-config** on page 301
- 1 **set radio-profile auto-tune channel-interval** on page 304
- 1 **show radio-profile** on page 408

set radio-profile auto-tune channel-interval

Sets the interval at which RF Auto-Tuning decides whether to change the channels on radios in a radio profile. At the end of each interval, UNIVERGE WL Control System processes the results of the RF scans performed during the previous interval, and changes radio channels if needed.

Syntax **set radio-profile** *name* **auto-tune channel-interval** *seconds*

<i>name</i>	Radio profile name.
<i>seconds</i>	Number of seconds RF Auto-Tuning waits before changing radio channels to adjust to RF changes, if needed. You can specify from 0 to 65535 seconds.

Defaults The default channel interval is 3600 seconds (one hour).

Access Enabled.

Usage It is recommended to use an interval of at least 300 seconds (5 minutes).

RF Auto-Tuning can change a radio channel before the channel interval expires in response to RF anomalies. Even in this case, channel changes cannot occur more frequently than the channel holddown interval.

If you set the interval to 0, RF Auto-Tuning does not reevaluate the channel at regular intervals. However, RF Auto-Tuning can still change the channel in response to RF anomalies.

Examples The following command sets the channel interval for radios in radio profile *rp2* to 2700 seconds (45 minutes):

```
PROPMT# set radio-profile rp2 auto-tune channel-interval 2700
success: change accepted.
```

See Also

- 1 **set radio-profile auto-tune channel-config** on page 301
- 1 **set radio-profile auto-tune channel-holddown** on page 303
- 1 **show radio-profile** on page 408

set radio-profile auto-tune power-config

Enables or disables dynamic power tuning (RF Auto-Tuning) for the UNIVERGE WL Access Points radios in a radio profile.

Syntax `set radio-profile name auto-tune power-config {enable | disable}`

<i>name</i>	Radio profile name.
enable	Configures radios to dynamically set their power levels when the UNIVERGE WL Access Points are started.
disable	Configures radios to use their statically assigned power levels, or the default power levels if unassigned, when the radios are started.

Defaults Dynamic power assignment is disabled by default.

Access Enabled.

Usage When RF Auto-Tuning for power is disabled, UNIVERGE WL Control System does not dynamically set the power levels when radios are first enabled and also does not tune power during operation with associated clients.

When RF Auto-Tuning for power is enabled, UNIVERGE WL Control System does not allow you to manually change the power level.

Examples The following command enables dynamic power tuning for radios in the *rp2* radio profile:

```
PROPMT# set radio-profile rp2 auto-tune power-config enable
success: change accepted.
```

See Also

- 1 **set ap radio auto-tune max-power** on page 292
- 1 **set radio-profile auto-tune channel-config** on page 301
- 1 **set radio-profile auto-tune power-interval** on page 306
- 1 **show radio-profile** on page 408

set radio-profile auto-tune power-interval

Sets the interval at which RF Auto-Tuning decides whether to change the power level on radios in a radio profile. At the end of each interval, UNIVERGE WL Control System processes the results of the RF scans performed during the previous interval, and changes radio power levels if needed.

Syntax **set radio-profile** *name* **auto-tune power-interval** *seconds*

<i>name</i>	Radio profile name.
<i>seconds</i>	Number of seconds UNIVERGE WL Control System waits before changing radio power levels to adjust to RF changes, if needed. You can specify from 1 to 65535 seconds.

Defaults The default power tuning interval is 300 seconds.

Access Enabled.

Examples The following command sets the power interval for radios in radio profile *rp2* to 240 seconds:

```
PROPMT# set radio-profile rp2 auto-tune power-interval 240
success: change accepted.
```

See Also

- 1 **set ap radio auto-tune max-power** on page 292
- 1 **set radio-profile auto-tune power-config** on page 305
- 1 **show service-profile** on page 413

set radio-profile beacon-interval

Changes the rate at which each AP radio in a radio profile advertises its service set identifier (SSID).

Syntax `set radio-profile name beacon-interval interval`

name Radio profile name.

interval Number of milliseconds (ms) between beacons. You can specify from 25 ms to 8191 ms.

Defaults The beacon interval for AP radios is 100 ms by default.

Access Enabled.

Usage You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

Examples The following command changes the beacon interval for radio profile *rp1* to 200 ms:

```
PROPMT# set radio-profile rp1 beacon-interval 200
success: change accepted.
```

See Also

- 1 **set radio-profile mode** on page 316
- 1 **show radio-profile** on page 408

set radio-profile countermeasures



Caution! Countermeasures affect wireless service on a radio. When an AP radio is sending countermeasures, the radio is disabled for use by network traffic, until the radio finishes sending the countermeasures.

Enables or disables countermeasures on the UNIVERGE WL Access Points radios managed by a radio profile. Countermeasures are packets sent by a radio to prevent clients from being able to use rogue access points.

set radio-profile countermeasures

Chapter 12

UNIVERGE WL Access Points radios can also issue countermeasures against interfering devices. An interfering device is not part of the UNIVERGE WL Control System but also is not a rogue. No client connected to the device has been detected communicating with any network entity listed in the forwarding database (FDD) of any UNIVERGE WL Controller in the Mobility Domain. Although the interfering device is not connected to your network, the device might be causing RF interference with UNIVERGE WL Access Points radios.

Syntax **set radio-profile** *name* **countermeasures** {**all** | **rogue** | **configured** | **none**}

<i>name</i>	Radio profile name.
all	Configures radios to attack rogues and interfering devices.
rogue	Configures radios to attack rogues only.
configured	Configures radios to attack only devices in the attack list on the UNIVERGE WL Controller (<i>on-demand</i> countermeasures). When this option is specified, devices found to be rogues by other means, such as policy violations or by determining that the device is providing connectivity to the wired network, are not attacked.
none	Disables countermeasures for this radio profile.

Defaults Countermeasures are disabled by default.

Access Enabled.

Examples The following command enables countermeasures in radio profile *radprof3* for rogues only:

```
PROPMT# set radio-profile radprof3 countermeasures rogue
success: change accepted.
```

The following command disables countermeasures in radio profile *radprof3*:

```
PROPMT# clear radio-profile radprof3 countermeasures
success: change accepted.
```

The following command causes radios managed by radio profile *radprof3* to issue countermeasures against devices in the UNIVERGE WL Controllers attack list:

```
PROPMT# set radio-profile radprof3 countermeasures configured
```

success: change accepted.

Note that when you issue this command, countermeasures are then issued only against devices in the UNIVERGE WL Controller attack list, not against other devices that were classified as rogues by other means.

See Also `show radio-profile` on page 408

set radio-profile dtim-interval

Changes the number of times after every beacon that each AP radio in a radio profile sends a delivery traffic indication map (DTIM). An AP sends the multicast and broadcast frames stored in its buffers to clients who request them in response to the DTIM.



Note. The DTIM interval applies to both the beacons SSID and the nonbeacons SSID.

Syntax `set radio-profile name dtim-interval interval`

name Radio profile name.

interval Number of times the DTIM is transmitted after every beacon. You can enter a value from 1 through 31.

Defaults By default, AP send the DTIM once after each beacon.

Access Enabled.

Usage You must disable all radios using a radio profile before you can change parameters in the profile. Use the `set radio-profile mode` command.

The DTIM interval does not apply to unicast frames.

Examples The following command changes the DTIM interval for radio profile *rp1* to 2:

```
PROPMT# set radio-profile rp1 dtim-interval 2
success: change accepted.
```

See Also

- 1 **set radio-profile mode** on page 316
- 1 **show radio-profile** on page 408

set radio-profile frag-threshold

Changes the fragmentation threshold for the AP radios in a radio profile. The fragmentation threshold is the threshold at which the long-retry-count is applicable instead of the short-retry-count.

The long-retry-count specifies the number of times a radio can send a unicast frame that is equal to or longer than the frag-threshold without receiving an acknowledgment.

The short-retry-count specifies the number of times a radio can send a unicast frame that is shorter than the frag-threshold without receiving an acknowledgment.

Syntax **set radio-profile** *name* **frag-threshold** *threshold*

name Radio profile name.

threshold Maximum frame length, in bytes. You can enter a value from 256 through 2346.

Defaults The default fragmentation threshold for AP radios is 2346 bytes.

Access Enabled.

Usage You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

The frag-threshold does not specify the maximum length a frame is allowed to be without being broken into multiple frames before transmission. The UNIVERGE WL Access Point does not support fragmentation upon transmission, only upon reception.

The frag-threshold does not change the RTS threshold, which specifies the maximum length of a frame before the radio uses the RTS/CTS method to send the frame. To change the RTS threshold, use the **set radio-profile rts-threshold** command instead.

Examples The following command changes the fragmentation threshold for radio profile *rp1* to 1500 bytes:

```
PROPMT# set radio-profile rp1 frag-threshold 1500
success: change accepted.
```

See Also

- 1 **set radio-profile mode** on page 316
- 1 **show radio-profile** on page 408

set radio-profile max-rx-lifetime

Changes the maximum receive threshold for the AP radios in a radio profile. The maximum receive threshold specifies the number of milliseconds that a frame *received* by a radio can remain in buffer memory.

Syntax **set radio-profile** *name* **max-rx-lifetime** *time*

<i>name</i>	Radio profile name.
<i>time</i>	Number of milliseconds. You can enter a value from 500 (0.5 second) through 250,000 (250 seconds).

Defaults The default maximum receive threshold for AP radios is 2000 ms (2 seconds).

Access Enabled.

Usage You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

Examples The following command changes the maximum receive threshold for radio profile *rp1* to 4000 ms:

```
PROPMT# set radio-profile rp1 max-rx-lifetime 4000
success: change accepted.
```

See Also

- 1 **set radio-profile mode** on page 316
- 1 **set radio-profile max-tx-lifetime** on page 312
- 1 **show radio-profile** on page 408

set radio-profile max-tx-lifetime

Changes the maximum transmit threshold for the AP radios in a radio profile. The maximum transmit threshold specifies the number of milliseconds that a frame *scheduled to be transmitted* by a radio can remain in buffer memory.

Syntax **set radio-profile** *name* **max-tx-lifetime** *time*

name Radio profile name.

time Number of milliseconds. You can enter a value from 500 (0.5 second) through 250,000 (250 seconds).

Defaults The default maximum transmit threshold for AP radios is 2000 ms (2 seconds).

Access Enabled.

Usage You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

Examples The following command changes the maximum transmit threshold for radio profile *rp1* to 4000 ms:

```
PROPM1# set radio-profile rp1 max-tx-lifetime 4000
success: change accepted.
```

See Also

- 1 **set radio-profile mode** on page 316
- 1 **set radio-profile max-rx-lifetime** on page 311
- 1 **show radio-profile** on page 408

set radio-profile max-voip-bw

Specifies the amount of bandwidth to reserve for active NEC handset calls on a radio.



Note. This command is equivalent to the **set radio-profile max-voip-sessions** command. (See “Usage”.)

Syntax **set radio-profile** *name* **max-voip-bw** *Kbps*

name Radio profile name.

Kbps Aggregate amount of bandwidth, in Kbps, to reserve for all voice sessions on individual radios. You can specify from 0 to 6000.

Defaults The default is 3000 Kbps.

Access Enabled.

Usage This command applies only to radio profiles with QoS mode **voice-extension**.

This command is equivalent to the **set radio-profile max-voip-sessions** command. Both commands reserve aggregate bandwidth on a radio profile's radios for NEC handsets. In fact, the **set radio-profile max-voip-sessions** command is not saved when you save the configuration. Instead, the command is translated into the equivalent **set radio-profile max-voip-bw** command, which is saved in the configuration.

Examples The following command reserves 200 Kbps for VoIP sessions for NEC handsets. This amount will be reserved on each radio in radio profile *rp1*:

```
PROPMT# set radio-profile rp1 max-voip-bw 200
success: max-voip-bw is 200 Kb/s
       min-client-rate: 1.0 Mb/s
       effective bandwidth: 500 Kb/s
```

Table 32 describes the fields in this display.

Table 32. Output for set radio-profile max-voip-bw

Field	Description
max-voip-bw	Amount of aggregate bandwidth to reserve on each radio.
min-client-rate	<p>Lowest mandatory 802.11g transmit rate configured on service profiles mapped to this radio profile. (Another term for this parameter is the <i>nominal rate</i>.)</p> <p>If no service profiles have been mapped to the radio profile or the CAC mode is not set to voice-extension in any of them, the following message is displayed:</p> <p>WARNING: cac-mode is not voice-ext in any service profiles</p>
effective bandwidth	<p>Maximum aggregate amount of bandwidth that can be used on a radio by voice sessions. This is the estimated amount of a radio's total bandwidth that will remain available after overhead such as the following:</p> <ul style="list-style-type: none">• 802.11 overhead, including retransmissions• VoIP control packet overhead including RTCP, and proprietary call/handset controls <p>If the aggregate bandwidth is more than the effective bandwidth, the following message is displayed:</p> <p>WARNING: max-voip-bw is more than effective bandwidth!</p> <p>This is not an error condition and UNIVERGE WL Control System will allow the configuration. However, it will be possible for a radio to become oversubscribed, which can reduce voice quality.</p>

See Also

- 1 **set radio-profile max-voip-sessions** on page 315
- 1 **set service-profile cac-mode** on page 341
- 1 **show radio-profile** on page 408

set radio-profile max-voip-sessions

Specifies the amount of bandwidth to reserve for active NEC handset calls on a radio.



Note. This command is equivalent to the **set radio-profile max-voip-bw** command. (See “Usage”.)

Syntax **set radio-profile** *name* **max-voip-sessions** *max-sessions* **codec** {**g.711** | **g.729**} **sample-period** {**10** | **20** | **30** | **40**}

<i>name</i>	Radio profile name.
<i>max-sessions</i>	Maximum number of active sessions to allow on a radio. You can specify from 1 to 30.
codec { g.711 g.729 }	Compression and decompression scheme used for voice sessions.
sample-period { 10 20 30 40 }	The interval, in milliseconds (ms), at which samples are transmitted.

Defaults This command has no defaults.

Access Enabled.

Usage This command applies only to radio profiles with QoS mode **voice-extension**.

This command is equivalent to the **set radio-profile max-voip-sessions** command. Both commands reserve aggregate bandwidth on a radio profile's radios for NEC handsets. In fact, the **set radio-profile max-voip-sessions** command is not saved when you save the configuration. Instead, the command is translated into the equivalent **set radio-profile max-voip-bw** command, which is saved in the configuration.

Examples The following command reserves bandwidth for a maximum of 4 active sessions per radio in the *rp1* radio profile, using codec g.711 with sample rate 10 ms:

```
PROPMT# set radio-profile rp1 max-voip-sessions 4 codec g.711 sample-period 10
success: max-voip-bw is 486 Kb/s
```

set radio-profile mode

Chapter 12

```
min-client-rate: 11.0 Mb/s
effective bandwidth: 6000 Kb/s
```



Note. For information about the output, see Table 32 on page 314. The output fields are the same as those for the **set radio-profile max-voip-bw** command.

See Also

- 1 **set radio-profile max-voip-bw** on page 313
- 1 **set service-profile cac-mode** on page 341
- 1 **show radio-profile** on page 408

set radio-profile mode

Creates a new radio profile, and disables or reenables all AP radios that are using a specific profile.

Syntax **set radio-profile** *name* [**mode** {**enable** | **disable**}]

radio-profile <i>name</i>	Radio profile name of up to 16 alphanumeric characters, with no spaces. Use this command without the mode enable or mode disable option to create a new profile.
mode enable	Enables the radios that use this profile.
mode disable	Disables the radios that use this profile.

Defaults Each radio profile that you create has a set of properties with factory default values that you can change with the other **set radio-profile** commands in this chapter. Table 33 lists the parameters controlled by a radio profile and their default values.

Table 33. Defaults for Radio Profile Parameters

Parameter	Default Value	Radio Behavior When Parameter Set To Default Value
active-scan	enable	Sends <i>probe any</i> requests (probe requests with a null SSID name) to solicit probe responses from other access points.
auto-tune	enable	Allows dynamic configuration of channel and power settings by UNIVERGE WL Control System.
beacon-interval	100	Waits 100 ms between beacons.
countermeasures	Not configured	Does not issue countermeasures against any device.
dtim-interval	1	Sends the delivery traffic indication map (DTIM) after every beacon.
frag-threshold	2346	Uses the short-retry-count for frames shorter than 2346 bytes and uses the long-retry-count for frames that are 2346 bytes or longer.
max-rx-lifetime	2000	Allows a received frame to stay in the buffer for up to 2000 ms (2 seconds).
max-tx-lifetime	2000	Allows a frame that is scheduled for transmission to stay in the buffer for up to 2000 ms (2 seconds).

Table 33. Defaults for Radio Profile Parameters

Parameter	Default Value	Radio Behavior When Parameter Set To Default Value
max-voip-bw	3000	Reserves an aggregate of 3000 Kbps on each radio for NEC VoIP sessions. Note: This parameter applies only when the QoS mode is voice-extension .
max-voip-sessions	Not configured	This parameter is equivalent to max-voip-bw and is never saved in the configuration. Instead, UNIVERGE WL Control System converts it into max-voip-bw before saving the configuration.
preamble-length	short	Advertises support for short 802.11b preambles, accepts either short or long 802.11b preambles, and generates unicast frames with the preamble length specified by the client. Note: This parameter applies only to 802.11b/g radios.
qos-mode	wmm	Classifies and marks traffic based on 802.1p and DSCP, and optimizes forwarding prioritization of AP radios for Wi-Fi Multimedia (WMM).
rfid-mode	disable	Radio does not function as a location receiver in an AeroScout Visibility System.

Table 33. Defaults for Radio Profile Parameters

Parameter	Default Value	Radio Behavior When Parameter Set To Default Value
rts-threshold	2346	Transmits frames longer than 2346 bytes by means of the Request-to-Send/Clear-to-Send (RTS/CTS) method.
service-profile	No service profiles defined	You must configure a service profile. The service profile sets the SSID name and other parameters.
wmm-powersave	disable	Requires clients to send a separate PSpoll to retrieve each unicast packet buffered by the UNIVERGE WL Access Points radio.

Access Enabled.

Usage Use the command without any optional parameters to create new profile. If the radio profile does not already exist, UNIVERGE WL Control System creates a new radio profile. Use the **enable** or **disable** option to enable or disable all the radios using a profile. To assign the profile to one or more radios, use the **set ap radio radio-profile** command.

To change a parameter in a radio profile, you must first disable all the radios in the profile. After you complete the change, you can reenable the radios.

To enable or disable specific radios without disabling all of them, use the **set ap radio** command.

Examples The following command configures a new radio profile named *rp1*:

```
PROPMT# set radio-profile rp1
success: change accepted.
```

The following command enables the radios that use radio profile *rp1*:

```
PROPMT# set radio-profile rp1 mode enable
```

set radio-profile preamble-length

Chapter 12

The following commands disable the radios that use radio profile *rp1*, change the beacon interval, then reenables the radios:

```
PROPMT# set radio-profile rp1 mode disable
PROPMT# set radio-profile rp1 beacon-interval 200
PROPMT# set radio-profile rp1 mode enable
```

The following command enables the WPA IE on AP radios in radio profile *rp2*:

```
PROPMT# set radio-profile rp2 wpa-ie enable
success: change accepted.
```

See Also

- 1 **set ap radio mode** on page 295
- 1 **set ap radio radio-profile** on page 296
- 1 **show ap config** on page 374
- 1 **show radio-profile** on page 408

set radio-profile preamble-length

Changes the preamble length for which an 802.11b/g AP radio advertises support. This command does not apply to 802.11a.

Syntax **set radio-profile** *name* **preamble-length** {**long** | **short**}

<i>name</i>	Radio profile name.
long	Advertises support for long preambles.
short	Advertises support for short preambles.

Defaults The default is **short**.

Access Enabled.

Usage Changing the preamble length value affects only the support advertised by the radio. Regardless of the preamble length setting (**short** or **long**), an 802.11b/g radio accepts and can generate 802.11b/g frames with either short or long preambles.

If a client associated with an 802.11b/g radio uses long preambles for unicast traffic, the UNIVERGE WL Access Point still accepts frames with short preambles but does not transmit frames with short preambles. This change also occurs if the access point overhears a beacon from an 802.11b/g radio on another access point that indicates the radio has clients that require long preambles.

You must disable all radios that use a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

Examples The following command configures 802.11b/g radios that use the radio profile *rp_long* to advertise support for long preambles instead of short preambles:

```
PROPMT# set radio-profile rp_long preamble-length long
success: change accepted.
```

See Also

- 1 **set radio-profile mode** on page 316
- 1 **show radio-profile** on page 408

set radio-profile qos-mode

Sets the prioritization mode for forwarding queues on UNIVERGE WL Access Points radios managed by the radio profile.

Syntax **set radio-profile** *name* **qos-mode** {**svp** | **voice-extension** | **wmm**}

svp	Optimizes forwarding prioritization of UNIVERGE WL Access Points radios for SpectraLink Voice Priority (SVP).
voice-extension	Optimizes forwarding prioritization of UNIVERGE WL Access Points radios for NEC handsets.
wmm	Classifies and marks traffic based on 802.1p and DSCP, and optimizes forwarding prioritization of UNIVERGE WL Access Points radios for Wi-Fi Multimedia (WMM).

Defaults The default QoS mode is **wmm**.

set radio-profile rate-enforcement

Chapter 12

Access Enabled.

Usage If you plan to use SVP, you also must configure an ACL to mark CoS in SVP traffic. (See the “Enabling Prioritization for Legacy Voice over IP” section in the “Configuring and Managing Security ACLs” chapter of the [Configuration Guide](#).)

Examples The following command changes the QoS mode for radio profile *rp1* to SVP:

```
PROPMT# set radio-profile rp1 qos-mode svp
success: change accepted.
```

See Also

1 **set radio-profile mode** on page 316

1 **show radio-profile** on page 408

set radio-profile rate-enforcement

Configures UNIVERGE WL Control System to enforce data rates, which means that a connecting client must transmit at one of the mandatory or standard rates in order to associate with the UNIVERGE WL Access Point.

Syntax **set radio-profile** *name* **rate-enforcement** {**enable** | **disable**}

<i>name</i>	Radio profile name.
enable	Enables data rate enforcement for the radios in the radio profile.
disable	Disables data rate enforcement for the radios in the radio profile.

Defaults Data rate enforcement is disabled by default.

Access Enabled.

Usage Each type of radio (802.11a, 802.11b, and 802.11g) providing service to an SSID has a set of radio rates allowed for use when sending beacons, multicast frames, and unicast data. You can configure the rate set for each type of radio, specifying rates in three categories:

- 1 Mandatory — Valid 802.11 transmit rates that clients must support in order to associate with the UNIVERGE WL Access Point
- 1 Disabled — Valid 802.11 transmit rates are disabled. UNIVERGE WL Access Points do not transmit at the disabled rates
- 1 Standard — Valid 802.11 transmit rates that are not disabled and are not mandatory

By default, the rate set is not enforced, meaning that a client can associate with and transmit data to the UNIVERGE WL Access Point using a disabled data rate, although the UNIVERGE WL Access Point does not transmit data back to the client at the disabled rate.

You can use this command to enforce the data rates, which means that a connecting client *must* transmit at one of the mandatory or standard rates in order to associate with the UNIVERGE WL Access Point. When data rate enforcement is enabled, clients transmitting at the disabled rates are not allowed to associate with the UNIVERGE WL Access Point.

This command is useful if you want to completely prevent clients from transmitting at disabled data rates. For example, you can disable slower data rates so that clients transmitting at these rates do not consume bandwidth on the channel at the expense of clients transmitting at faster rates.

Examples The following command enables data rate enforcement for radio profile *rp1*:

```
PROPM1# set radio-profile rp1 rate-enforcement mode enable
success: change accepted.
```

See Also

- 1 **set service-profile transmit-rates** on page 362
- 1 **show ap counters** on page 378

set radio-profile rts-threshold

Changes the RTS threshold for the AP radios in a radio profile. The RTS threshold specifies the maximum length a frame can be before the radio uses the RTS/CTS method to send the frame. The RTS/CTS method clears the air of other traffic to avoid corruption of the frame due to a collision with another frame.

set radio-profile service-profile

Chapter 12

Syntax **set radio-profile** *name* **rts-threshold** *threshold*

<i>name</i>	Radio profile name.
<i>threshold</i>	Maximum frame length, in bytes. You can enter a value from 256 through 3000.

Defaults The default RTS threshold for an AP radio is 2346 bytes.

Access Enabled.

Usage You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

Examples The following command changes the RTS threshold for radio profile *rp1* to 1500 bytes:

```
PROPMT# set radio-profile rp1 rts-threshold 1500
success: change accepted.
```

See Also

- 1 **set radio-profile mode** on page 316
- 1 **show radio-profile** on page 408

set radio-profile service-profile

Maps a service profile to a radio profile. All radios that use the radio profile also use the parameter settings, including SSID and encryption settings, in the service profile.

Syntax **set radio-profile** *name* **service-profile** *name*

radio-profile <i>name</i>	Radio profile name of up to 16 alphanumeric characters, with no spaces.
service-profile <i>name</i>	Service profile name of up to 16 alphanumeric characters, with no spaces.

Defaults A radio profile does not have a service profile associated with it by default. In this case, the radios in the radio profile use the default settings for parameters controlled by the service profile. Table 34 lists the parameters controlled by a service profile and their default values.

Table 34. Defaults for Service Profile Parameters

Parameter	Default Value	Radio Behavior When Parameter Set To Default Value
active-call-idle-timeout	120	Releases the bandwidth reserved for an active NEC voice session (on-hook call), if the session remains idle for 120 seconds.
attr	No attributes configured	Does not assign the SSID's authorization attribute values to SSID users, even if attributes are not otherwise assigned.
auth-dot1x	enable	When the Wi-Fi Protected Access (WPA) information element (IE) is enabled, uses 802.1X to authenticate WPA clients.
auth-fallthru	none	Denies access to users who do not match an 802.1X or MAC authentication rule for the SSID requested by the user.
auth-psk	disable	Does not support using a preshared key (PSK) to authenticate WPA clients.
beacon	enable	Sends beacons to advertise the SSID managed by the service profile.

Table 34. Defaults for Service Profile Parameters

Parameter	Default Value	Radio Behavior When Parameter Set To Default Value
cac-mode	none	Does not limit the number of active user sessions based on Call Admission Control (CAC).
cac-session	12	If session-based CAC is enabled (cac-mode is set to session), limits the number of active user sessions on a radio to 14.
cipher-ccmp	disable	Does not use Counter with Cipher Block Chaining Message Authentication Code Protocol (CCMP) to encrypt traffic sent to WPA clients.
cipher-tkip	enable	When the WPA IE is enabled, uses Temporal Key Integrity Protocol (TKIP) to encrypt traffic sent to WPA clients.
cipher-wep104	disable	Does not use Wired Equivalent Privacy (WEP) with 104-bit keys to encrypt traffic sent to WPA clients.
cipher-wep40	disable	Does not use WEP with 40-bit keys to encrypt traffic sent to WPA clients.
cos	0	If static CoS is enabled (static-cos is set to enable), assigns CoS 0 to all data traffic to or from clients.

Table 34. Defaults for Service Profile Parameters

Parameter	Default Value	Radio Behavior When Parameter Set To Default Value
dhcp-restrict	disable	Does not restrict a client's traffic to only DHCP traffic while the client is being authenticated and authorized.
idle-client-probing	enable	Sends a keepalive packet (a null-data frame) to each client every 10 seconds.
keep-initial-vlan	disable	Reassigns the user to a VLAN after roaming, instead of leaving the roamed user on the VLAN assigned by the switch where the user logged on. Note: Enabling this option does not retain the initial VLAN assignment for a user in all cases. (For information, see “set service-profile keep-initial-vlan” on page 350.)
long-retry-count	5	Sends a long unicast frame up to five times without acknowledgment.
no-broadcast	disable	Does not reduce wireless broadcast traffic by sending unicasts to clients for ARP requests and DHCP Offers and Acks instead of forwarding them as multicasts.
proxy-arp	enable	Replies on behalf of wireless clients to ARP requests for client IP addresses, instead of forwarding the ARP Requests as wireless broadcasts.

Table 34. Defaults for Service Profile Parameters

Parameter	Default Value	Radio Behavior When Parameter Set To Default Value
psk-phrase	No passphrase defined	Uses dynamically generated keys rather than statically configured keys to authenticate WPA clients.
psk-raw	No preshared key defined	Uses dynamically generated keys rather than statically configured keys to authenticate WPA clients.
rsn-ie	disable	Does not use the RSN IE in transmitted frames. (The RSN IE is required for 802.11i. RSN is sometimes called WPA2.)
shared-key-auth	disable	Does not use shared-key authentication. This parameter does not enable PSK authentication for WPA. To enable PSK encryption for WPA, use the set radio-profile auth-psk command.
short-retry-count	5	Sends a short unicast frame up to five times without acknowledgment.
ssid-type	crypto	Encrypts wireless traffic for the SSID.
static-cos	disable	Assigns CoS based on the QoS mode (voice-extension , wmm , or svp) or based on ACLs.

Table 34. Defaults for Service Profile Parameters

Parameter	Default Value	Radio Behavior When Parameter Set To Default Value
tkip-mc-time	60000	Uses Michael countermeasures for 60,000 ms (60 seconds) following detection of a second MIC failure within 60 seconds.
transmit-rates	802.11a: <ul style="list-style-type: none"> • mandatory: 6.0,12.0,24.0 • beacon-rate: 6.0 • multicast-rate: auto • disabled: none 802.11b: <ul style="list-style-type: none"> • mandatory: 5.5,11.0 • beacon-rate: 5.5 • multicast-rate: auto • disabled: none 802.11g: <ul style="list-style-type: none"> • mandatory: 1.0,2.0,5.5,11.0 • beacon-rate: 5.5 • multicast-rate: auto • disabled: none 	Accepts associations only from clients that support one of the mandatory rates. Sends beacons at the specified rate (6 Mbps for 802.11a, 5.5 Mbps for 802.11b/g). Sends multicast data at the highest rate that can reach all clients connected to the radio. Accepts frames from clients at all valid data rates. (No rates are disabled by default.)
user-idle-timeout	180	Allows a client to remain idle for 180 seconds (3 minutes) before UNIVERGE WL Control System changes the client's session to the Disassociated state.

Table 34. Defaults for Service Profile Parameters

Parameter	Default Value	Radio Behavior When Parameter Set To Default Value
web-portal-acl	portalacl Note: This is the default only if the fallthru type on the service profile has been set to web-portal . Otherwise, the value is unconfigured.	If set to portalacl and the service profile fallthru is set to web-portal , radios use the <i>portalacl</i> ACL to filter traffic for Web Portal users during authentication. If the fallthru type is web-portal but web-portal-acl is set to an ACL other than <i>portalacl</i> , the other ACL is used. If the fallthru type is not web-portal , radios do not use the web-portal-acl setting.
web-portal-form	Not configured	For Web Authentication users, serves the UNIVERGE WL Control System login page.
web-portal-session-timeout	5	Allows a Web Portal Web Authentication session to remain in the Deassociated state 5 seconds before being terminated automatically.
wep key-index	No keys defined	Uses dynamic WEP rather than static WEP. Note: If you configure a WEP key for static WEP, UNIVERGE WL Control System continues to also support dynamic WEP.

Table 34. Defaults for Service Profile Parameters

Parameter	Default Value	Radio Behavior When Parameter Set To Default Value
wep active-multicast-index	1	Uses WEP key 1 for static WEP encryption of multicast traffic if WEP encryption is enabled and keys are defined.
wep active-unicast-index	1	Uses WEP key 1 for static WEP encryption of unicast traffic if WEP encryption is enabled and keys are defined.
wpa-ie	disable	Does not use the WPA IE in transmitted frames.

Access Enabled.

Usage You must configure the service profile before you can map it to a radio profile. You can map the same service profile to more than one radio profile.

You must disable all radios that use a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

Examples The following command maps service-profile *wpa_clients* to radio profile *rp2*:

```
PROPMT# set radio-profile rp2 service-profile wpa_clients
success: change accepted.
```

See Also

- 1 **set service-profile active-call-idle-timeout** on page 333
- 1 **set service-profile attr** on page 334
- 1 **set service-profile auth-dot1x** on page 336
- 1 **set service-profile auth-fallthru** on page 337
- 1 **set service-profile auth-psk** on page 339
- 1 **set service-profile beacon** on page 340
- 1 **set service-profile cac-mode** on page 341

set radio-profile service-profile

Chapter 12

- 1 **set service-profile cac-session** on page 342
- 1 **set service-profile cipher-ccmp** on page 343
- 1 **set service-profile cipher-tkip** on page 343
- 1 **set service-profile cipher-wep104** on page 344
- 1 **set service-profile cipher-wep40** on page 346
- 1 **set service-profile cos** on page 347
- 1 **set service-profile dhcp-restrict** on page 348
- 1 **set service-profile idle-client-probing** on page 349
- 1 **set service-profile long-retry-count** on page 351
- 1 **set service-profile no-broadcast** on page 351
- 1 **set service-profile proxy-arp** on page 353
- 1 **set service-profile psk-phrase** on page 354
- 1 **set service-profile psk-raw** on page 355
- 1 **set service-profile rsn-ie** on page 356
- 1 **set service-profile shared-key-auth** on page 357
- 1 **set service-profile short-retry-count** on page 358
- 1 **set service-profile ssid-name** on page 359
- 1 **set service-profile ssid-type** on page 359
- 1 **set service-profile static-cos** on page 360
- 1 **set service-profile tkip-mc-time** on page 361
- 1 **set service-profile transmit-rates** on page 362
- 1 **set service-profile user-idle-timeout** on page 365
- 1 **set service-profile web-portal-form** on page 366
- 1 **set service-profile web-portal-session-timeout** on page 368
- 1 **set service-profile wep active-multicast-index** on page 369

- 1 **set service-profile wep active-unicast-index** on page 370
- 1 **set service-profile wep key-index** on page 371
- 1 **set service-profile wpa-ie** on page 372
- 1 **show radio-profile** on page 408
- 1 **show service-profile** on page 413

set service-profile active-call-idle-timeout

Changes the number of seconds UNIVERGE WL Control System will continue to reserve bandwidth for an active voice session (on-hook call). If the timer expires, the radio releases the bandwidth that was reserved for the session.

The timer is reset to 0 each time a client sends data or reregisters with its SIP server.

Syntax **set service-profile** *name* **active-call-idle-timeout** *seconds*

<i>name</i>	Service profile name.
<i>seconds</i>	<p>Number of seconds an on-hook client is allowed to remain idle before the radio UNIVERGE WL Control System releases the bandwidth reserved for the session. You can specify from 20 to 300 seconds. To disable the timer, specify 0.</p> <p>UNIVERGE WL Control System resets the timer by keepaliving between UNIVERGE WL Access Points and client.</p> <p>If you specify less than 60, active-call-idle-timeout happens, before the keepalive packets reach. And then bandwidth might release.</p> <p>UNIVERGE WL Control System recommends that you do not specify less than 60.</p>

Defaults The default active-call idle timeout is 120 seconds (2 minutes).

Access Enabled.

set service-profile attr

Chapter 12

Usage The active-call idle timeout applies only to active voice sessions (on-hook calls) on an SSID whose service profile has CAC mode **voice-extension** and whose radio profile has QoS mode **voice-extension**. For all other sessions, the user idle timeout applies instead. The user idle timeout also applies to sessions whose active-call idle timeout has expired.

Examples The following command increases the active-call idle timeout to 180 seconds (3 minutes) in service profile *sp1*:

```
PROPMT# set service-profile sp1 active-call-idle-timeout 180
success: change accepted.
```

See Also

- 1 **set service-profile user-idle-timeout** on page 365
- 1 **set service-profile web-portal-session-timeout** on page 368
- 1 **show service-profile** on page 413

set service-profile attr

Configures authorization attributes that are applied by default to users accessing the SSID managed by the service profile. These SSID default attributes are applied in addition to any supplied by the RADIUS server or from the local database.

Syntax **set service-profile** *name* **attr** *attribute-name value*

name Service profile name.

attribute-name value Name and value of an attribute you are using to authorize SSID users for a particular service or session characteristic.

For a list of authorization attributes and values that you can assign to network users, see Table 25 on page 223. All of the attributes listed in Table 25 can be used with this command except **ssid**.

Defaults By default, a service profile does not have any authorization attributes set.

Access Enabled.

Usage To change the value of a default attribute for a service profile, use the **set service-profile attr** command and specify a new value.

The SSID default attributes are applied *in addition* to any attributes supplied for the user by the RADIUS server or the local database. When the same attribute is specified both as an SSID default attribute and through AAA, then the attribute supplied by the RADIUS server or the local database takes precedence over the SSID default attribute. If a location policy is configured, the location policy rules also take precedence over SSID default attributes. The SSID default attributes serve as a fallback when neither the AAA process, nor a location policy, provides them.

For example, a service profile might be configured with the **service-type** attribute set to 2. If a user accessing the SSID is authenticated by a RADIUS server, and the RADIUS server returns the **vlan-name** attribute set to *orange*, then that user has a total of two attributes set: **service-type** and **vlan-name**.

If the service profile is configured with the **vlan-name** attribute set to *blue*, and the RADIUS server returns the **vlan-name** attribute set to *orange*, then the attribute from the RADIUS server takes precedence; the user is placed in the orange VLAN.

You can display the attributes for each connected user and if they are set through AAA or through SSID defaults by entering the **show sessions network verbose** command. You can display the configured SSID defaults by entering the **show service-profile** command.

Examples The following command assigns users accessing the SSID managed by service profile *sp2* to VLAN *blue*:

```
PROPMT# set service-prof sp2 attr vlan-name blue
success: change accepted.
```

The following command assigns users accessing the SSID managed by service profile *sp2* to the Mobility Profile *tulip*.

```
PROPMT# set service-prof sp2 attr mobility-profile tulip
success: change accepted.
```

set service-profile auth-dot1x

Chapter 12

The following command limits the days and times when users accessing the SSID managed by service profile *sp2* can access the network, to 5 p.m. to 2 a.m. every weekday, and all day Saturday and Sunday:

```
PROPMT# set service-prof sp2 attr time-of-day Wk1700-0200,Sa,Su
success: change accepted.
```

See Also

- 1 **show service-profile** on page 413
- 1 **show sessions network** on page 536

set service-profile auth-dot1x

Disables or reenables 802.1X authentication of Wi-Fi Protected Access (WPA) clients by UNIVERGE WL Access Points radios, when the WPA information element (IE) is enabled in the service profile that is mapped to the radio profile that the radios are using.

Syntax **set service-profile** *name* **auth-dot1x** {**enable** | **disable**}

<i>name</i>	Service profile name.
enable	Enables 802.1X authentication of WPA clients.
disable	Disables 802.1X authentication of WPA clients.

Defaults When the WPA IE is enabled, 802.1X authentication of WPA clients is enabled by default. If the WPA IE is disabled, the **auth-dot1x** setting has no effect.

Access Enabled.

Usage This command does not disable dynamic WEP for non-WPA clients. To disable dynamic WEP for non-WPA clients, enable the WPA IE (if not already enabled) and disable the 40-bit WEP and 104-bit WEP cipher suites in the WPA IE, if they are not already disabled.

To use 802.1X authentication for WPA clients, you also must enable the WPA IE.

If you disable 802.1X authentication of WPA clients, the only method available for authenticating the clients is preshared key (PSK) authentication. To use this, you must enable PSK support and configure a passphrase or key.

Examples The following command disables 802.1X authentication for WPA clients that use service profile *wpa_clients*:

```
PROPMT# set service-profile wpa_clients auth-dot1x disable
success: change accepted.
```

See Also

- 1 **set service-profile auth-psk** on page 339
- 1 **set service-profile psk-phrase** on page 354
- 1 **set service-profile wpa-ie** on page 372
- 1 **show service-profile** on page 413

set service-profile auth-fallthru

Specifies the authentication type for users who do not match an 802.1X or MAC authentication rule for an SSID managed by the service profile. When a user tries to associate with an SSID, UNIVERGE WL Control System checks the authentication rules for that SSID for a userglob that matches the username. If the SSID does not have an authentication rule that matches the username, authentication for the user *falls through* to the fallthru type.

The fallthru type is a service profile parameter, and applies to all radios within the radio profiles that are mapped to the service profile.

Syntax **set service-profile** *name* **auth-fallthru**
{**last-resort** | **none** | **web-portal**}

last-resort	Automatically authenticates the user and allows access to the SSID requested by the user, without requiring a username and password.
none	Denies authentication and prohibits the user from accessing the SSID. Note: The fallthru authentication type none is different from the authentication method none you can specify for administrative access. The fallthru authentication type none denies access to a network user. In contrast, the authentication method none allows access to the UNIVERGE WL Controller by an administrator. (See “set authentication admin” on page 203 and “set authentication console” on page 206.)
web-portal	Serves the user a web page from the UNIVERGE WL Controllers nonvolatile storage for secure login to the network.

Defaults The default fallthru authentication type is **none**.

If a username does not match a userglob in an authentication rule for the SSID requested by the user, the UNIVERGE WL Controller that is managing the radio the user is connected to redirects the user to a web page located on the UNIVERGE WL Controller. The user must type a valid username and password on the web page to access the SSID.

Access Enabled.

Usage The **last-resort** fallthru authentication type allows any user to access any SSID managed by the service profile. This method does not require the user to provide a username or password. Use the **last-resort** method only if none of the SSIDs managed by the service profile require secure access.

The **web-portal** authentication type also requires additional configuration items. (See the “Configuring AAA for Network Users” chapter of the [Configuration Guide](#).)

Examples The following command sets the fallthru authentication type for SSIDS managed by the service profile *rnd_lab* to web-portal:

```
PROPMT# set service-profile rnd_lab auth-fallthru web-portal
success: change accepted.
```

See Also

- 1 **set web-portal** on page 240
- 1 **set service-profile web-portal-form** on page 366
- 1 **show service-profile** on page 413

set service-profile auth-psk

Enables pre-shared key (PSK) authentication of Wi-Fi Protected Access (WPA) clients by UNIVERGE WL Access Points radios in a radio profile, when the WPA information element (IE) is enabled in the service profile.

Syntax `set service-profile name auth-psk {enable | disable}`

<i>name</i>	Service profile name.
enable	Enables PSK authentication of WPA clients.
disable	Disables PSK authentication of WPA clients.

Defaults When the WPA IE is enabled, PSK authentication of WPA clients is enabled by default. If the WPA IE is disabled, the **auth-psk** setting has no effect.

Access Enabled.

Usage This command affects authentication of WPA clients only.

To use PSK authentication, you also must configure a passphrase or key. In addition, you must enable the WPA IE.

Examples The following command enables PSK authentication for service profile *wpa_clients*:

```
PROPMT# set service-profile wpa_clients auth-psk enable
success: change accepted.
```

See Also

- 1 **set service-profile auth-dot1x** on page 336
- 1 **set service-profile psk-raw** on page 355
- 1 **set service-profile wpa-ie** on page 372
- 1 **show service-profile** on page 413

set service-profile beacon

Disables or reenables beaconing of the SSID managed by the service profile.

A UNIVERGE WL Access Point radio responds to an 802.11 *probe any* request with only the beaconned SSID(s). For a nonbeaconned SSID, radios respond only to directed 802.11 probe requests that match the nonbeaconned SSID's SSID string.

When you disable beaconing for an SSID, the radio still sends beacon frames, but the SSID name in the frames is blank.

Syntax **set service-profile** *name* **beacon** {**enable** | **disable**}

name Service profile name.

enable Enables beaconing of the SSID managed by the service profile.

disable Disables beaconing of the SSID managed by the service profile.

Defaults Beaconing is enabled by default.

Access Enabled.

Examples The following command disables beaconing of the SSID managed by service profile *sp2*:

```
PROPMT# set service-profile sp2 beacon disable
success: change accepted.
```

See Also

- 1 **set radio-profile beacon-interval** on page 307

- 1 **set service-profile ssid-name** on page 359
- 1 **set service-profile ssid-type** on page 359
- 1 **show service-profile** on page 413

set service-profile cac-mode

Configures the Call Admission Control (CAC) mode.

Syntax **set service-profile** *name* **cac-mode** { **none** | **session** | **voice-extension** }

<i>name</i>	Service profile name.
none	CAC is not used.
session	CAC is based on the number of active sessions.
voice-extension	CAC is based on the amount of reserved bandwidth available on UNIVERGE WL Access Points radios. Bandwidth that is in use by other voice sessions is not available for new sessions.

Defaults The default CAC mode is **none**.

Access Enabled.

Usage If you use **voice-extension**, you can change the amount of bandwidth reserved for each session, and the maximum number of sessions, using the **set radio-profile max-voip-bw** and **set radio-profile max-voip-sessions** commands.

If you use **session**, you can change the maximum number of active sessions a radio can have using the **set service-profile cac-session** command.

Examples The following command enables bandwidth-based CAC on service profile *sp1*:

```
PROPMT# set service-profile sp1 cac-mode voice-extension
success: change accepted.
```

See Also

- 1 **set radio-profile max-voip-bw** on page 313
- 1 **set radio-profile max-voip-sessions** on page 315

- 1 **set service-profile cac-session** on page 342
- 1 **show service-profile** on page 413

set service-profile cac-session

Specifies the maximum number of active sessions a radio can have when session-based CAC is enabled. When a UNIVERGE WL Access Point radio has reached the maximum allowed number of active sessions, the radio refuses connections from additional clients.

Syntax **set service-profile** *name* **cac-session** *max-sessions*

name Service profile name.

max-sessions Maximum number of active sessions allowed on the radio.

Defaults The default number of sessions allowed is 12.

Access Enabled.

Usage This command applies only when the CAC mode is **session**. If the CAC mode is **none**, you can still change the maximum number of sessions, but the setting does not take effect until you change the CAC mode to **session**. To change the CAC mode, use the **set service-profile cac-mode** command.

Examples The following command changes the maximum number of sessions for radios used by service profile *sp1* to 10:

```
PROPMT# set service-profile sp1 cac-session 10
success: change accepted.
```

See Also

- 1 **set service-profile cac-mode** on page 341
- 1 **show service-profile** on page 413

set service-profile cipher-ccmp

Enables Counter with Cipher Block Chaining Message Authentication Code Protocol (CCMP) encryption with WPA clients, for a service profile.

Syntax `set service-profile name cipher-ccmp {enable | disable}`

name Service profile name.

enable Enables CCMP encryption for WPA clients.

disable Disables CCMP encryption for WPA clients.

Defaults CCMP encryption is disabled by default.

Access Enabled.

Usage To use CCMP, you must also enable the WPA IE.

Examples The following command configures service profile *sp2* to use CCMP encryption:

```
PROPMY# set service-profile sp2 cipher-ccmp enable
success: change accepted.
```

See Also

- 1 **set service-profile cipher-tkip** on page 343
- 1 **set service-profile cipher-wep104** on page 344
- 1 **set service-profile cipher-wep40** on page 346
- 1 **set service-profile wpa-ie** on page 372
- 1 **show service-profile** on page 413

set service-profile cipher-tkip

Disables or reenables Temporal Key Integrity Protocol (TKIP) encryption in a service profile.

set service-profile cipher-wep104

Chapter 12

Syntax **set service-profile** *name* **cipher-tkip** {**enable** | **disable**}

<i>name</i>	Service profile name.
enable	Enables TKIP encryption for WPA clients.
disable	Disables TKIP encryption for WPA clients.

Defaults When the WPA IE is enabled, TKIP encryption is enabled by default.

Access Enabled.

Usage To use TKIP, you must also enable the WPA IE.

Examples The following command disables TKIP encryption in service profile *sp2*:

```
PROPMT# set service-profile sp2 cipher-tkip disable
success: change accepted.
```

See Also

- 1 **set service-profile cipher-ccmp** on page 343
- 1 **set service-profile cipher-wep104** on page 344
- 1 **set service-profile cipher-wep40** on page 346
- 1 **set service-profile tkip-mc-time** on page 361
- 1 **set service-profile wpa-ie** on page 372
- 1 **show service-profile** on page 413

set service-profile cipher-wep104

Enables dynamic Wired Equivalent Privacy (WEP) with 104-bit keys, in a service profile.

Syntax **set service-profile** *name* **cipher-wep104** {**enable** | **disable**}

<i>name</i>	Service profile name.
-------------	-----------------------

enable Enables 104-bit WEP encryption for WPA clients.
disable Disables 104-bit WEP encryption for WPA clients.

Defaults 104-bit WEP encryption is disabled by default.

Access Enabled.

Usage To use 104-bit WEP with WPA clients, you must also enable the WPA IE.

When 104-bit WEP in WPA is enabled in the service profile, radios managed by a radio profile that is mapped to the service profile can also support non-WPA clients that use dynamic WEP.

To support WPA clients that use 40-bit dynamic WEP, you must enable WEP with 40-bit keys. Use the **set service-profile cipher-wep40** command.

Microsoft Windows XP does not support WEP with WPA. To configure a service profile to provide dynamic WEP for XP clients, leave WPA disabled and use the **set service-profile wep** commands.

To support non-WPA clients that use static WEP, you must configure static WEP keys. Use the **set service-profile wep key-index** command.

Examples The following command configures service profile *sp2* to use 104-bit WEP encryption:

```
PROPMT# set service-profile sp2 cipher-wep104 enable
success: change accepted.
```

See Also

- 1 **set service-profile cipher-ccmp** on page 343
- 1 **set service-profile cipher-tkip** on page 343
- 1 **set service-profile cipher-wep40** on page 346
- 1 **set service-profile wep key-index** on page 371
- 1 **set service-profile wpa-ie** on page 372
- 1 **show service-profile** on page 413

set service-profile cipher-wep40

Enables dynamic Wired Equivalent Privacy (WEP) with 40-bit keys, in a service profile.

Syntax **set service-profile** *name* **cipher-wep40** {**enable** | **disable**}

name Service profile name.

enable Enables 40-bit WEP encryption for WPA clients.

disable Disables 40-bit WEP encryption for WPA clients.

Defaults 40-bit WEP encryption is disabled by default.

Access Enabled.

Usage To use 40-bit WEP with WPA clients, you must also enable the WPA IE.

When 40-bit WEP in WPA is enabled in the service profile, radios managed by a radio profile that is mapped to the service profile can also support non-WPA clients that use dynamic WEP.

To support WPA clients that use 104-bit dynamic WEP, you must enable WEP with 104-bit keys in the service profile. Use the **set service-profile cipher-wep104** command.

Microsoft Windows XP does not support WEP with WPA. To configure a service profile to provide dynamic WEP for XP clients, leave WPA disabled and use the **set service-profile wep** commands.

To support non-WPA clients that use static WEP, you must configure static WEP keys. Use the **set service-profile wep key-index** command.

Examples The following command configures service profile *sp2* to use 40-bit WEP encryption:

```
PROPM1# set service-profile sp2 cipher-wep40 enable
success: change accepted.
```

See Also

- 1 **set service-profile cipher-ccmp** on page 343
- 1 **set service-profile cipher-tkip** on page 343
- 1 **set service-profile cipher-wep104** on page 344
- 1 **set service-profile wep key-index** on page 371
- 1 **set service-profile wpa-ie** on page 372
- 1 **show service-profile** on page 413

set service-profile cos

Sets the Class-of-Service (CoS) level for static CoS.

Syntax **set service-profile** *name* **cos** *level*

name Service profile name.

level CoS value assigned by the UNIVERGE WL Access Points to all traffic in the service profile.

Defaults The default static CoS level is 0.

Access Enabled.

Usage This command applies only when static CoS is enabled. If static CoS is disabled, prioritization is based on the QoS mode configured in the radio profile, and on any ACLs that set CoS. (See the “Configuring Quality of Service” chapter of the [Configuration Guide](#).) To enable static CoS, use the **set service-profile static-cos** command.

Examples The following command changes the static CoS level to 7 (voice priority):

```
PROPMT# set service-profile sp1 cos 7
success: change accepted.
```

See Also

- 1 **set service-profile static-cos** on page 360
- 1 **show service-profile** on page 413

set service-profile dhcp-restrict

Enables or disables DHCP Restrict on a service profile. DHCP Restrict filters the traffic from a newly associated client and allows DHCP traffic only, until the client has been authenticated and authorized. All other traffic is captured by the UNIVERGE WL Controller and is not forwarded. After the client is successfully authorized, the traffic restriction is removed.

Syntax **set service-profile** *name* **dhcp-restrict** {**enable** | **disable**}

<i>name</i>	Service profile name.
enable	Enables DHCP Restrict.
disable	Disables DHCP Restrict.

Defaults DHCP Restrict is disabled by default.

Access Enabled.

Usage To further reduce the overhead of DHCP traffic, use the **set service-profile no-broadcast** command to disable DHCP broadcast traffic from UNIVERGE WL Access Points radios to clients on the service profile's SSID.

Examples The following command enables DHCP Restrict on service profile *sp1*:

```
PROPMT# set service-profile sp1 dhcp-restrict enable
success: change accepted.
```

See Also

- 1 **set service-profile no-broadcast** on page 351
- 1 **set service-profile proxy-arp** on page 353
- 1 **show service-profile** on page 413

set service-profile idle-client-probing

Disables or reenables periodic keepalives from UNIVERGE WL Access Points radios to clients on a service profile's SSID. When idle-client probing is enabled, the UNIVERGE WL Access Points radio sends a unicast null-data frame to each client every 10 seconds. Normally, a client that is still active sends an Ack in reply to the keepalive.

If a client does not send any data or respond to any keepalives before the user idle timeout expires, UNIVERGE WL Control System changes the client session to the Disassociated state.

Syntax `set service-profile name idle-client-probing {enable | disable}`

name Service profile name.

enable Enables keepalives.

disable Disables keepalives.

Defaults Idle-client probing is enabled by default.

Access Enabled.

Usage The length of time a client can remain idle (unresponsive to idle-client probes) is specified by the **user-idle-timeout** command.

Examples The following command disables idle-client keepalives on service profile *sp1*:

```
PROPMT# set service-profile sp1 idle-client-probing disable
success: change accepted.
```

See Also

- 1 **set service-profile user-idle-timeout** on page 365
- 1 **show service-profile** on page 413

set service-profile keep-initial-vlan

Configures UNIVERGE WL Access Point radios managed by the radio profile to leave a roamed user on the VLAN assigned by the UNIVERGE WL Controller where the user logged on. When this option is disabled, a users VLAN is reassigned by each UNIVERGE WL Controller when a user roams.

Syntax `set service-profile name keep-initial-vlan { enable | disable }`

<i>name</i>	Service profile name.
enable	Enables radios to leave a roamed user on the same VLAN instead of reassigning the VLAN.
disable	Configures radios to reassign a roamed user VLAN.

Defaults This option is disabled by default. Be sure to set as **enable**.

Access Enabled.

Usage Even when this option is enabled, the UNIVERGE WL Controller to which a user roams (the *roamed-to* switch) can reassign the VLAN in any of the following cases:

- 1 A location policy on the local switch reassigns the VLAN.
- 1 The user is configured in the switch's local database and the VLAN-Name attribute is set on the user or on a user group the user is in.
- 1 The access rule on the roamed-to switch uses RADIUS, and the VLAN-Name attribute is set on the RADIUS server.

Examples The following command enables the **keep-initial-vlan** option on service profile *sp3*:

```
PROPMT# set service-profile sp3 keep-initial-vlan enable
success: change accepted.
```

See Also `show service-profile` on page 413

set service-profile long-retry-count

Changes the long retry threshold for a service profile. The long retry threshold specifies the number of times a radio can send a long unicast frame without receiving an acknowledgment. A long unicast frame is a frame that is equal to or longer than the frag-threshold.

Syntax `set service-profile name long-retry-count threshold`

name Service profile name.

threshold Number of times the radio can send the same long unicast frame. You can enter a value from 1 through 15.

Defaults The default long unicast retry threshold is 5 attempts.

Access Enabled.

Examples The following command changes the long retry threshold for service profile *sp1* to 8:

```
PROPMT# set service-profile sp1 long-retry-count 8
success: change accepted.
```

See Also

- 1 **set radio-profile frag-threshold** on page 310
- 1 **set service-profile short-retry-count** on page 358
- 1 **show service-profile** on page 413

set service-profile no-broadcast

Disables or reenables the no-broadcast mode. The no-broadcast mode helps reduce traffic overhead on an SSID by having more SSID bandwidth available for unicast traffic. The no-broadcast mode also helps VoIP handsets conserve power by reducing the amount of broadcast traffic sent to the phones.

When enabled, the no-broadcast mode prevents UNIVERGE WL Access Points radios from sending DHCP or ARP broadcasts to clients on the service profile SSID. Instead, a UNIVERGE WL Access Point radio handles this traffic as follows:

set service-profile no-broadcast

Chapter 12

- 1 ARP requests—If the SSID has clients with IP addresses that the UNIVERGE WL Controller does not already know, the UNIVERGE WL Controller allows the UNIVERGE WL Access Points radio to send the ARP request as a unicast to only those stations whose addresses the UNIVERGE WL Controller does not know. The UNIVERGE WL Access Points radio does not forward the ARP request as a broadcast and does not send the request as a unicast to stations whose addresses the UNIVERGE WL Controller already knows.
- 1 DHCP Offers or Acks—If the destination MAC address belongs to a client on the SSID, the UNIVERGE WL Access Points radio sends the DHCP Offer or Ack as a unicast to that client only.

The no-broadcast mode does not affect other types of broadcast traffic and does not prevent clients from sending broadcasts.

Syntax **set service-profile** *name* **no-broadcast** {**enable** | **disable**}

<i>name</i>	Service profile name.
enable	Enables the no-broadcast mode. UNIVERGE WL Access Points radios are not allowed to send broadcast traffic to clients on the service profile's SSID.
disable	Disables the no-broadcast mode.

Defaults The no-broadcast mode is disabled by default. (Broadcast traffic not disabled.)

Access Enabled.

Usage To further reduce traffic on a service profile, use the **set service-profile dhcp-restrict** command to capture non-DHCP traffic to and from clients who are still in the authentication or authorization process.

Examples The following command enables the no-broadcast mode on service profile *sp1*:

```
PROPMT# set service-profile sp1 no-broadcast enable
success: change accepted.
```

See Also

- 1 **set service-profile dhcp-restrict** on page 348
- 1 **set service-profile proxy-arp** on page 353

1 **show service-profile** on page 413

set service-profile proxy-arp

Disables or reenables proxy ARP. When proxy ARP is enabled, the UNIVERGE WL Controller replies to ARP requests for client IP address on behalf of the clients. This feature reduces broadcast overhead on a service profile SSID by eliminating ARP broadcasts from UNIVERGE WL Access Points radios to the SSID's clients.

If the ARP request is for a client with an IP address that UNIVERGE WL Controller does not already have, the UNIVERGE WL Controller allows UNIVERGE WL Access Points radios to send the ARP request to clients. If the no-broadcast mode is also enabled, the UNIVERGE WL Access Points radios send the ARP request as a unicast to only the clients whose addresses the UNIVERGE WL Controller does not know. However, if no-broadcast mode is disabled, the UNIVERGE WL Access Points radios sends the ARP request as a broadcast to all clients on the SSID.

Syntax **set service-profile** *name* **proxy-arp** { **enable** | **disable** }

name Service profile name.

enable Enables proxy ARP.

disable Disables proxy ARP.

Defaults Proxy ARP is enabled by default.

Access Enabled.

Usage To further reduce broadcast traffic on a service profile, use the **set service-profile no-broadcast** command to disable DHCP and ARP request broadcasts.

Examples The following command disables proxy ARP on service profile *sp1*:

```
PROPMT# set service-profile sp1 proxy-arp disable
success: change accepted.
```

See Also

1 **set service-profile dhcp-restrict** on page 348

- 1 **set service-profile no-broadcast** on page 351
- 1 **show service-profile** on page 413

set service-profile psk-phrase

Configures a passphrase for preshared key (PSK) authentication to use for authenticating WPA clients, in a service profile. Radios use the PSK as a pairwise master key (PMK) to derive unique pairwise session keys for individual WPA clients.

Syntax `set service-profile name psk-phrase passphrase`

<i>name</i>	Service profile name.
<i>passphrase</i>	An ASCII string from 8 to 63 characters long. The string can contain blanks if you use quotation marks at the beginning and end of the string.

Defaults None.

Access Enabled.

Usage UNIVERGE WL Control System converts the passphrase into a 256-bit binary number for system use and a raw hexadecimal key to store in the UNIVERGE WL Controller configuration. Neither the binary number nor the passphrase itself is ever displayed in the configuration.

To use PSK authentication, you must enable it and you also must enable the WPA IE.

Examples The following command configures service profile *sp3* to use passphrase “1234567890123<>?+=&% The quick brown fox jumps over the lazy sl”:

```
PROPMT# set service-profile sp3 psk-phrase "1234567890123<>?+=&% The quick  
brown fox jumps over the lazy sl"  
success: change accepted.
```

See Also

- 1 **set mac-user attr** on page 222

- 1 **set service-profile auth-psk** on page 339
- 1 **set service-profile psk-raw** on page 355
- 1 **set service-profile wpa-ie** on page 372
- 1 **show service-profile** on page 413

set service-profile psk-raw

Configures a raw hexadecimal preshared key (PSK) to use for authenticating WPA clients, in a service profile. Radios use the PSK as a pairwise master key (PMK) to derive unique pairwise session keys for individual WPA clients.

Syntax **set service-profile** *name* **psk-raw** *hex*

<i>name</i>	Service profile name.
<i>hex</i>	A 64-bit ASCII string representing a 32-digit hexadecimal number. Enter the two-character ASCII form of each hexadecimal number.

Defaults None.

Access Enabled.

Usage UNIVERGE WL Control System converts the hexadecimal number into a 256-bit binary number for system use. UNIVERGE WL Control System also stores the hexadecimal key in the UNIVERGE WL Controller configuration. The binary number is never displayed in the configuration.

To use PSK authentication, you must enable it and you also must enable WPA IE.

Examples The following command configures service profile *sp3* to use a raw PSK with PSK clients:

```
PROPMT# set service-profile sp3 psk-raw
c25d3fe4483e867d1df96eaacdf8b02451fa0836162e758100f5f6b87965e59d
success: change accepted.
```

See Also

- 1 **set mac-user attr** on page 222
- 1 **set service-profile auth-psk** on page 339
- 1 **set service-profile psk-phrase** on page 354
- 1 **set service-profile wpa-ie** on page 372
- 1 **show service-profile** on page 413

set service-profile rsn-ie

Enables the Robust Security Network (RSN) Information Element (IE).

The RSN IE advertises the RSN (sometimes called WPA2) authentication methods and cipher suites supported by radios in the radio profile mapped to the service profile.

Syntax **set service-profile** *name* **rsn-ie** {**enable** | **disable**}

<i>name</i>	Service profile name.
enable	Enables the RSN IE.
disable	Disables the RSN IE.

Defaults The RSN IE is disabled by default.

Access Enabled.

Usage When the RSN IE is enabled, the default authentication method is 802.1X. There is no default cipher suite. You must enable the cipher suites you want the radios to support.

Examples The following command enables the RSN IE in service profile *sprsn*:

```
PROPM1# set service-profile sprsn rsn-ie enable
success: change accepted.
```

See Also

- 1 **set service-profile auth-dot1x** on page 336

- 1 **set service-profile auth-psk** on page 339
- 1 **set service-profile cipher-ccmp** on page 343
- 1 **set service-profile cipher-wep104** on page 344
- 1 **set service-profile cipher-wep40** on page 346
- 1 **show service-profile** on page 413

set service-profile shared-key-auth

Enables shared-key authentication, in a service profile.



Note. Use this command only if advised to do so by UNIVERGE WL Control System. This command does not enable preshared key (PSK) authentication for Wi-Fi Protected Access (WPA). To enable PSK encryption for WPA, use the **set service-profile auth-psk** command.

Syntax **set service-profile** *name* **shared-key-auth** { **enable** | **disable** }

<i>name</i>	Service profile name.
enable	Enables shared-key authentication.
disable	Disables shared-key authentication.

Defaults Shared-key authentication is disabled by default.

Access Enabled.

Usage Shared-key authentication is supported only for encrypted SSIDs. In addition, if you enable shared-key authentication, RSN, WPA, TKIP, and CCMP must be disabled. By default, RSN, WPA, and CCMP are already disabled, but TKIP is enabled; you must manually disable TKIP. To disable TKIP, use the **set service-profile cipher-tkip disable** command.

Examples The following command enables shared-key authentication in service profile *sp4*:

```
PROPMT# set service-profile sp4 shared-key-auth enable
success: change accepted.
```

set service-profile short-retry-count

Chapter 12

See Also

- 1 **set radio-profile mode** on page 316
- 1 **set service-profile cipher-tkip** on page 343
- 1 **show service-profile** on page 413

set service-profile short-retry-count

Changes the short retry threshold for a service profile. The short retry threshold specifies the number of times a radio can send a short unicast frame without receiving an acknowledgment. A short unicast frame is a frame that is shorter than the frag-threshold.

Syntax **set service-profile** *name* **short-retry-count** *threshold*

name Service profile name.

threshold Number of times a radio can send the same short unicast frame. You can enter a value from 1 through 15.

Defaults The default short unicast retry threshold is 5 attempts.

Access Enabled.

Examples The following command changes the short retry threshold for service profile *sp1* to 3:

```
PROPMPT# set service-profile sp1 short-retry-count 3
success: change accepted.
```

See Also

- 1 **set radio-profile frag-threshold** on page 310
- 1 **set service-profile long-retry-count** on page 351
- 1 **show service-profile** on page 413

set service-profile ssid-name

Configures the SSID name in a service profile.

Syntax `set service-profile name ssid-name ssid-name`

<i>name</i>	Service profile name.
<i>ssid-name</i>	Name of up to 32 alphanumeric characters. You can include blank spaces in the name, if you delimit the name with single or double quotation marks. You must use the same type of quotation mark (either single or double) on both ends of the string.

Defaults The default SSID type is crypto (encrypted) .

Access Enabled.

Examples The following command applies the name *guest* to the SSID managed by service profile *clear_wlan*:

```
PROPMT# set service-profile clear_wlan ssid-name guest
success: change accepted.
```

The following command applies the name *corporate users* to the SSID managed by service profile *mycorp_srvcprf*:

```
PROPMT# set service-profile mycorp_srvcprf ssid-name "corporate users"
success: change accepted.
```

See Also

- 1 **set service-profile ssid-type** on page 359
- 1 **show service-profile** on page 413

set service-profile ssid-type

Specifies whether the SSID managed by a service profile is encrypted or unencrypted.

set service-profile static-cos

Chapter 12

Syntax **set service-profile** *name* *ssid-type* [**clear** | **crypto**]

<i>name</i>	Service profile name.
clear	Wireless traffic for the service profile's SSID is not encrypted.
crypto	Wireless traffic for the service profile's SSID is encrypted.

Defaults The default SSID type is crypto.

Access Enabled.

Examples The following command changes the SSID type for service profile *clear_wlan* to **clear**:

```
PROPMT# set service-profile clear_wlan ssid-type clear
success: change accepted.
```

See Also

- 1 **set service-profile ssid-name** on page 359
- 1 **show service-profile** on page 413

set service-profile static-cos

Enables or disables static CoS on a service profile. Static CoS assigns the same CoS level to all traffic on the service profile's SSID, regardless of 802.1p or DSCP markings in the packets themselves, and regardless of any ACLs that mark CoS. This option provides a simple way to configure an SSID for priority traffic such as VoIP traffic.

When static CoS is enabled, the standard UNIVERGE WL Control System prioritization mechanism is not used. Instead, the UNIVERGE WL Access Points sets CoS as follows:

- 1 For traffic from the UNIVERGE WL Access Points to clients, the UNIVERGE WL Access Points places the traffic into the forwarding queue that corresponds to the CoS level configured on the service profile. For example, if the static CoS level is set to 7, the UNIVERGE WL Access Points radio places client traffic in its Voice queue.

- 1 For traffic from clients to the network, the UNIVERGE WL Access Points marks the DSCP value in the IP headers of the tunnel packets used to carry the user data from the UNIVERGE WL Access Points to the UNIVERGE WL Controller.

Syntax `set service-profile name static-cos {enable | disable}`

name Service profile name.
enable Enables static CoS on the service profile.
disable Disables static CoS on the service profile.

Defaults Static CoS is disabled by default.

Access Enabled.

Usage The CoS level is specified by the `set service-profile cos` command. The default static CoS level is 0 (low priority).

Examples The following command enables static CoS on service profile *sp1*:

```
PROPMT# set service-profile sp1 static-cos enable
success: change accepted.
```

See Also

- 1 `set service-profile cos` on page 347
- 1 `show service-profile` on page 413

set service-profile tkip-mc-time

Changes the length of time that UNIVERGE WL Access Points radios use countermeasures if two message integrity code (MIC) failures occur within 60 seconds. When countermeasures are in effect, UNIVERGE WL Access Points radios dissociate all TKIP and WPA WEP clients and refuse all association and reassociation requests until the countermeasures end.

set service-profile transmit-rates

Chapter 12

Syntax `set service-profile name tkip-mc-time wait-time`

name Service profile name.

wait-time Number of milliseconds (ms) countermeasures remain in effect. You can specify from 0 to 60,000.

Defaults The default countermeasures wait time is 60,000 ms (60 seconds).

Access Enabled.

Usage Countermeasures apply only to TKIP and WEP clients. This includes WPA WEP clients and non-WPA WEP clients. CCMP clients are not affected.

The TKIP cipher suite must be enabled. The WPA IE also must be enabled.

Examples The following command changes the countermeasures wait time for service profile *sp3* to 30,000 ms (30 seconds):

```
PROPMT# set service-profile sp3 tkip-mc-time 30000
success: change accepted.
```

See Also

- 1 **set service-profile cipher-tkip** on page 343
- 1 **set service-profile wpa-ie** on page 372
- 1 **show service-profile** on page 413

set service-profile transmit-rates

Changes the data rates supported by UNIVERGE WL Access Points radios for a service-profile SSID.

Syntax `set service-profile name transmit-rates { 11a | 11b | 11g } mandatory rate-list [disabled rate-list] [beacon-rate rate] [multicast-rate { rate | auto }]`

name Service profile name.

11a | **11b** | **11g** Radio type.

mandatory *rate-list*

Set of data transmission rates that clients are required to support in order to associate with an SSID on a UNIVERGE WL Access Point radio. A client must support at least one of the mandatory rates.

These rates are advertised in the basic rate set of 802.11 beacons, probe responses, and reassociation response frames sent by UNIVERGE WL Access Points radios.

Data frames and management frames sent by UNIVERGE WL Access Points radios use one of the specified mandatory rates.

The valid rates depend on the radio type:

- **11a**—6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0
- **11b**—1.0, 2.0, 5.5, 11.0
- **11g**—1.0, 2.0, 5.5, 6.0, 9.0, 11.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0

Use a comma to separate multiple rates; for example: **6.0,9.0,12.0**

disabled *rate-list*

Data transmission rates that UNIVERGE WL Access Points radios do not use to transmit data.

This setting applies only to data sent by the UNIVERGE WL Access Points radios. The radios still accepts frames from clients at disabled data rates.

The valid rates depend on the radio type and are the same as the valid rates for **mandatory**.

beacon-rate <i>rate</i>	<p>Data rate of beacon frames sent by UNIVERGE WL Access Points radios.</p> <p>The valid rates depend on the radio type and are the same as the valid rates for mandatory. However, you cannot set the beacon rate to a disabled rate.</p> <p>Note: UNIVERGE WL Access Points radios send probe-response frames using the transit rates at which they are received.</p>
multicast-rate { <i>rate</i> auto }	<p>Data rate of multicast frames sent by UNIVERGE WL Access Points radios.</p> <ul style="list-style-type: none"> • <i>rate</i>—Sets the multicast rate to a specific rate. The valid rates depend on the radio type and are the same as the valid rates for mandatory. However, you cannot set the multicast rate to a disabled rate. • auto—Sets the multicast rate to the highest rate that can reach all clients connected to the UNIVERGE WL Access Points radio.

Defaults This command has the following defaults:

- 1 **mandatory:**
 - 1 **11a—6.0,12.0,24.0**
 - 1 **11b—5.5,11.0**
 - 1 **11g—1.0,2.0,5.5,11.0**
- 1 **disabled**—None. All rates applicable to the radio type are supported by default.
- 1 **beacon-rate:**
 - 1 **11a—6.0**
 - 1 **11b—5.5**
 - 1 **11g—5.5**
- 1 **multicast-rate—auto** for all radio types.

Access Enabled.

Usage If you disable a rate, you cannot use the rate as a mandatory rate or the beacon or multicast rate. All rates that are applicable to the radio type and that are not disabled are supported by the radio.

Examples The following command sets 802.11a mandatory rates for service profile *sp1* to 6 Mbps and 9 Mbps, disables rates 48 Mbps and 54 Mbps, and changes the beacon rate to 9 Mbps:

```

PROPMT# set service-profile sp1 transmit-rates 11a mandatory 6.0,9.0 disabled
        48.0,54.0 beacon-rate 9.0
success: change accepted.

```

See Also

- 1 **show service-profile** on page 413
- 1 **set radio-profile rate-enforcement** on page 322

set service-profile user-idle-timeout

Changes the number of seconds UNIVERGE WL Control System leaves a session up for a client that is not sending data and is not responding to keepalives (idle-client probes). If the timer expires, the client session is changed to the Dissociated state.

The timer is reset to 0 each time a client sends data or responds to an idle-client probe. If the idle-client probe is disabled, the timer is reset each time the client sends data.

Syntax **set service-profile** *name* **user-idle-timeout** *seconds*

<i>name</i>	Service profile name.
<i>seconds</i>	Number of seconds a client is allowed to remain idle before UNIVERGE WL Control System changes the session to the Dissociated state. You can specify from 20 to 86400 seconds. To disable the timer, specify 0.

Defaults The default user idle timeout is 180 seconds (3 minutes).

set service-profile web-portal-form

Chapter 12

Access Enabled.

Usage The user idle timeout does not apply to active voice sessions (on-hook calls) on an SSID whose service profile has CAC mode **voice-extension** and whose radio profile has QoS mode **voice-extension**. The active-call idle timeout (set by the **set service-profile active-call-idle-timeout** command) applies to these sessions instead.

Examples The following command increases the user idle timeout to 360 seconds (6 minutes) in service profile *sp1*:

```
PROPMT# set service-profile sp1 user-idle-timeout 360  
success: change accepted.
```

See Also

- 1 **set service-profile active-call-idle-timeout** on page 333
- 1 **set service-profile idle-client-probing** on page 349
- 1 **set service-profile web-portal-session-timeout** on page 368
- 1 **show service-profile** on page 413

set service-profile web-portal-form

Specifies a custom login page that loads for Web Authentication users requesting the SSID managed by the service profile.

Syntax **set service-profile** *name* **web-portal-form** *url*

name Service profile name.

url UNIVERGE WL Controller subdirectory name and HTML page name of the login page. Specify the full path. For example, *corpa-ssid/corpa.html*.

Defaults The UNIVERGE WL Control System Web login page is served by default.

Access Enabled.

Usage It is recommended that you create a subdirectory for the custom page and place all of the files for the page in that subdirectory. Do not place the custom page in the root directory of the UNIVERGE WL Controller user file area.

If the custom login page includes gif or jpg images, their path names are interpreted relative to the directory from which the page is served.



Note. To use Web Authentication, the fallback authentication type in the service profile that manages the SSID must be set to **web-portal**.

The **web-portal** authentication type also requires additional configuration items. (See the “Configuring AAA for Network Users” chapter of the [Configuration Guide](#).)

Examples The following commands create a subdirectory named *corpa*, copy a custom login page named *corpa-login.html* and a jpg image named *corpa-logo.jpg* into that subdirectory, and set the Web login page for service profile *corpa-service* to *corpa-login.html*:

```

PROPMT# mkdir corpa
success: change accepted.

PROPMT# copy tftp://10.1.1.1/corpa-login.html corpa/corpa-login.html
success: received 637 bytes in 0.253 seconds [ 2517 bytes/sec]

PROPMT# copy tftp://10.1.1.1/corpa-logo.jpg corpa/corpa-logo.jpg
success: received 1202 bytes in 0.402 seconds [ 2112 bytes/sec]

PROPMT# dir corpa
=====
file:
Filename                               Size      Created
file:corpa-login.html                  637 bytes  Aug 12 2004, 15:42:26
file:corpa-logo.jpg                    1202 bytes  Aug 12 2004, 15:57:11
Total: 1839 bytes used, 206577 Kbytes free

PROPMT# set service-profile corpa-service web-portal-form corpa/corpa-login.html
success: change accepted.

```

See Also

- 1 **copy** on page 581
- 1 **dir** on page 584
- 1 **mkdir** on page 589
- 1 **set service-profile auth-fallthru** on page 337

- 1 **set web-portal** on page 240
- 1 **show service-profile** on page 413

set service-profile web-portal-session-timeout

Changes the number of seconds UNIVERGE WL Control System allows Web Portal Web Authentication sessions to remain in the Deassociated state before being terminated automatically.

Syntax **set service-profile** *name* **web-portal-session-timeout** *seconds*

<i>name</i>	Service profile name.
<i>seconds</i>	Number of seconds UNIVERGE WL Control System allows Web Portal Web Authentication sessions to remain in the Deassociated state before being terminated automatically. You can specify from 5 to 2800 seconds.

Defaults The default Web Portal Web Authentication session timeout is 5 seconds.

Access Enabled.

Usage When a client that has connected through Web Portal Web Authentication enters standby or hibernation mode, the client may be idle for longer than the User idle-timeout period. When the User idle-timeout period expires, UNIVERGE WL Control System places the client Web Portal Web Authentication session in the Deassociated state. The Web Portal Web Authentication session can remain in the Deassociated state for a configurable amount of time before being terminated automatically. This configurable amount of time is called the Web Portal Web Authentication session timeout period. You can use this command to set the number of seconds in the Web Portal Web Authentication session timeout period.

Note that the Web Portal Web Authentication session timeout period applies only to Web Portal Web Authentication sessions already authenticated with a username and password. For all other Web Portal Web Authentication sessions, the default Web Portal Web Authentication session timeout period of 5 seconds is used.

Examples The following command allows Web Portal Web Authentication sessions to remain in the Deassociated state 180 seconds before being terminated automatically.

```
PROPMT# set service-profile sp1 web-portal-session-timeout 180
success: change accepted.
```

See Also

- 1 **set service-profile user-idle-timeout** on page 365
- 1 **show service-profile** on page 413

set service-profile wep active-multicast-index

Specifies the static Wired-Equivalent Privacy (WEP) key (one of four) to use for encrypting multicast frames.

Syntax `set service-profile name wep active-multicast-index num`

name Service profile name.

num WEP key number. You can enter a value from 1 through 4.

Defaults If WEP encryption is enabled and WEP keys are defined, AP radios use WEP key 1 to encrypt multicast frames, by default.

Access Enabled.

Usage Before using this command, you must configure values for the WEP keys you plan to use. Use the **set service-profile wep key-index** command.

Examples The following command configures service profile *sp2* to use WEP key 2 for encrypting multicast traffic:

```
PROPMT# set service-profile sp2 wep active-multicast-index 2
success: change accepted.
```

See Also

- 1 **set service-profile wep active-unicast-index** on page 370
- 1 **set service-profile wep key-index** on page 371
- 1 **show service-profile** on page 413

set service-profile wep active-unicast-index

Specifies the static Wired-Equivalent Privacy (WEP) key (one of four) to use for encrypting unicast frames.

Syntax **set service-profile** *name* **wep active-unicast-index** *num*

name Service profile name.

num WEP key number. You can enter a value from 1 through 4.

Defaults If WEP encryption is enabled and WEP keys are defined, AP radios use WEP key 1 to encrypt unicast frames, by default.

Access Enabled.

Usage Before using this command, you must configure values for the WEP keys you plan to use. Use the **set service-profile wep key-index** command.

Examples The following command configures service profile *sp2* to use WEP key 4 for encrypting unicast traffic:

```
PROPMT# set service-profile sp2 wep active-unicast-index 4
success: change accepted.
```

See Also

- 1 **set service-profile wep active-multicast-index** on page 369
- 1 **set service-profile wep key-index** on page 371
- 1 **show service-profile** on page 413

set service-profile wep key-index

Sets the value of one of four static Wired-Equivalent Privacy (WEP) keys for static WEP encryption.

Syntax `set service-profile name wep key-index num key value`

<i>name</i>	Service profile name.
key-index <i>num</i>	WEP key index. You can enter a value from 1 through 4.
key <i>value</i>	Hexadecimal value of the key. You can enter a 10-character ASCII string representing a 5-byte hexadecimal number or a 26-character ASCII string representing a 13-byte hexadecimal number. You can use numbers or letters. ASCII characters in the following ranges are supported: <ul style="list-style-type: none">• 0 to 9• A to F• a to f

Defaults By default, no static WEP keys are defined.

Access Enabled.

Usage UNIVERGE WL Control System automatically enables static WEP when you define a WEP key. UNIVERGE WL Control System continues to support dynamic WEP.

Examples The following command configures a 5-byte WEP key for key index 1 on service profile *sp2* to *aabbccdde*:

```
PROPMT# set service-profile sp2 wep key-index 1 key aabbccdde  
success: change accepted.
```

See Also

- 1 **set service-profile wep active-multicast-index** on page 369
- 1 **set service-profile wep active-unicast-index** on page 370
- 1 **show service-profile** on page 413

set service-profile wpa-ie

Enables the WPA information element (IE) in wireless frames. The WPA IE advertises the WPA authentication methods and cipher suites supported by radios in the radio profile mapped to the service profile.

Syntax `set service-profile name wpa-ie {enable | disable}`

name Service profile name.

enable Enables the WPA IE.

disable Disables the WPA IE.

Defaults The WPA IE is disabled by default.

Access Enabled.

Usage When the WPA IE is enabled, the default authentication method is 802.1X. There is no default cipher suite. You must enable the cipher suites you want the radios to support.

Examples The following command enables the WPA IE in service profile *sp2*:

```
PROPMI# set service-profile sp2 wpa-ie enable
success: change accepted.
```

See Also

- 1 **set service-profile auth-dot1x** on page 336
- 1 **set service-profile auth-psk** on page 339
- 1 **set service-profile cipher-ccmp** on page 343
- 1 **set service-profile cipher-tkip** on page 343
- 1 **set service-profile cipher-wep104** on page 344
- 1 **set service-profile cipher-wep40** on page 346
- 1 **show service-profile** on page 413

show ap acl hits



Note. This command is not supported.

show ap acl map



Note. This command is not supported.

show ap acl resource-usage



Note. This command is not supported.

show ap arp



Note. This command is not supported.

show ap config

Displays global and radio-specific settings for an AP.

Syntax **show ap config** [*ap-number* [**radio** {**1** | **2**}]]

<i>ap-number</i>	Index value that identifies the UNIVERGE WL Access Points on the UNIVERGE WL Controller.
radio 1	Shows configuration information for radio 1.
radio 2	Shows configuration information for radio 2. (This option does not apply to single-radio models.)

Defaults None.

Access Enabled.

Usage UNIVERGE WL Control System lists information for AP.

Examples The following example shows configuration information for an AP configured on connection 2:

```
PROPMT# show ap config 2
AP 2: serial-id: 123456789, AP model: WL1500-AP, bias: high, name: AP02
upgrade-firmware: YES
force-image-download: NO
communication timeout: 10
location:
contact:
Radio 1: type: 802.11g, mode: disabled, channel: dynamic
tx pwr: 18, profile: default
auto-tune max-power: default,
load-balance-group: ,
load-balance-enable: YES,
force-rebalance: NO,
local-switching: disabled, vlan-profile: default
```

Table 35 describes the fields in this display.

Table 35. Output for show ap config

Field	Description
AP	Index number that identifies the UNIVERGE WL Access Points on the switch.
serial-id	Serial ID of the AP.
AP model	AP model number.
bias	Bias of the UNIVERGE WL Controller connection to the AP: <ul style="list-style-type: none"> • High • Low
name	AP name, if configured.
upgrade-firmware	State of the firmware upgrade option: <ul style="list-style-type: none"> • YES (automatic upgrades are enabled) • NO (automatic upgrades are disabled)
force-image-download	State of the option to force the UNIVERGE WL Access Points to download its software image from the UNIVERGE WL Controller instead of loading the image that is locally stored on the UNIVERGE WL Access Points.
communication timeout	
location	Location information for the UNIVERGE WL Access Points.
contact	Contact information for the UNIVERGE WL Access Points.
Radio	Radio number. The information listed below this field applies specifically to the radio.
type	Radio type: <ul style="list-style-type: none"> • 802.11a • 802.11b • 802.11g

Table 35. Output for show ap config

Field	Description
mode	Radio state: <ul style="list-style-type: none"> • Enabled • Disabled
channel	Channel number.
antennatype	External antenna model, if applicable.
tx pwr	Transmit power, in dBm.
profile	Radio profile that manages the radio. Until you assign the radio to a radio profile, UNIVERGE WL Control System assigns the radio to the default radio profile.
auto-tune max-power	Maximum power level the RF Auto-Tuning feature can set on the radio. <ul style="list-style-type: none"> • The value <i>default</i> means RF Auto-Tuning can set the power up to the maximum level allowed for the country of operation. • A specific numeric value means you or another administrator set the maximum value.
load-balance-group	Names of the RF load-balancing groups to which the UNIVERGE WL Access Point belongs. If the value is <i>None</i> , the access point does not belong to any load balancing groups. <p>Note: This field is displayed only if the UNIVERGE WL Access Point is a member of a group.</p>
load-balance-enable	Whether RF load balancing is enabled for this UNIVERGE WL Access Point.
force-rebalance	Whether the UNIVERGE WL Access Points radio to disassociates its client sessions and rebalance them whenever a new UNIVERGE WL Access Point radio is added to the RF load balancing group.

Table 35. Output for show ap config

Field	Description
local-switching	Whether local packet switching is enabled for the UNIVERGE WL Access Points.
vlan-profile	The VLAN profile the UNIVERGE WL Access Point uses for local packet switching, indicating which VLANs are locally switched.

See Also

- 1 **set ap** on page 54
- 1 **set ap bias** on page 282
- 1 **set ap fingerprint** on page 288
- 1 **set ap name** on page 290
- 1 **set ap upgrade-firmware** on page 300
- 1 **set ap radio mode** on page 295
- 1 **set ap radio antennatype** on page 291
- 1 **set ap radio channel** on page 293
- 1 **set ap radio radio-profile** on page 296
- 1 **set ap radio tx-power** on page 297
- 1 **show ap connection** on page 403
- 1 **show ap global** on page 405
- 1 **show ap unconfigured** on page 407
- 1 **show radio-profile** on page 408

show ap counters

Displays AP and radio statistics counters.

Syntax `show ap counters [ap-number [radio {1 | 2}]]`

ap-number Index value that identifies the UNIVERGE WL Access Points on the UNIVERGE WL Controller.

radio 1 Shows statistics counters for radio 1.

radio 2 Shows statistics counters for radio 2. (This option does not apply to single-radio models.)

Defaults None.

Access Enabled.

Usage To display statistics counters and other information for individual user sessions, use the **show sessions network** command.

Examples The following command shows statistics counters for UNIVERGE WL Access Points 7:

PROPMT# `show ap counters 7`

```
AP: 7          radio: 1
=====
LastPktXferRate      2          PktTxCount      73473
NumCntInPwrSave      0          MultiPktDrop    0
LastPktRxSigStrength -89         MultiBytDrop    0
LastPktSigNoiseRatio  4          User Sessions   0
TKIP Pkt Transfer Ct  0          MIC Error Ct   0
TKIP Pkt Replays     0          TKIP Decrypt Err 0
CCMP Pkt Decrypt Err  0          CCMP Pkt Replays 0
CCMP Pkt Transfer Ct  0          RadioResets     0
Radio Recv Phy Err Ct 0          Transmit Retries 60501
Radio Adjusted Tx Pwr 15         Noise Floor     -93
802.3 Packet Tx Ct   0          802.3 Packet Rx Ct 0
No Receive Descriptor 0          Illegal Rates

          TxUniPkt  TxUniByte      RxPkt      UndcrptPkt
          TxMultiPkt TxMultiByte RxByte      UndcrptByte
                                PhyErr
1.0: 1017      0 10170      0 14 8347      0 0 3964
2.0: 5643 55683 822545 8697520 3 1670      0 0 8695
5.5: 0         0 0         0 5 258      0 0 4
```

```

6.0: 0 0 0 0 0 0 0 0 0 51
9.0: 0 0 0 0 0 1 172 0 0 53
11.0: 0 0 0 0 0 17 998 0 0 35
12.0: 0 0 0 0 0 0 0 0 0 26
18.0: 0 0 0 0 0 0 0 0 0 38
24.0: 0 0 0 0 0 0 0 0 0 47
36.0: 0 0 0 0 0 0 0 0 0 1
48.0: 0 0 0 0 0 1 68 0 0 29
54.0: 0 0 0 0 0 0 0 0 0 5
TOTL: 6660 55683 832715 8697520 41 11513 0 0 12948
...
```

Table 36 describes the fields in this display.

Table 36. Output for show ap counters

Field	Description
AP	UNIVERGE WL Access Points number.
radio	Radio number.
LastPktXferRate	Data transmit rate, in Mbps, of the last packet received by the AP.
NumCntInPwrSave	Number of clients currently in power save mode.
LastPktRxSigStrength	Signal strength, in dBm, of the last packet received by the AP.
LastPktSigNoiseRatio	Signal-to-noise ratio (SNR), in decibels (dB), of the last packet received by the AP. This value indicates the strength of the radio signal above the noise floor. For example, if the noise floor is -88 and the signal strength is -68, the SNR is 20. If the value is below 10, this indicates a weak signal and might indicate a problem in the RF environment.
TKIP Pkt Transfer Ct	Total number of TKIP packets sent and received by the radio.

Table 36. Output for show ap counters

Field	Description
TKIP Pkt Replays	<p>Number of TKIP packets that were resent to the UNIVERGE WL Access Points by a client.</p> <p>A low value (under about one hundred) does not necessarily indicate a problem. However, if this counter is increasing steadily or has a very high value (in the hundreds or more), a Denial of Service (DoS) attack might be occurring. Contact UNIVERGE.</p>
CCMP Pkt Decrypt Err	<p>Number of times a decryption error occurred with a packet encrypted with CCMP.</p> <p>Occasional decryption errors do not indicate a problem.</p> <p>However, steadily increasing errors or a high number of errors can indicate that data loss is occurring in the network. Generally, this is caused by a key mismatch between a client and the UNIVERGE WL Access Points. To locate the client that is experiencing decryption errors (and therefore is likely causing this counter to increment on the UNIVERGE WL Access Points), use the show sessions network session-id session-id command for each client on the radio.</p> <p>After you identify the client that is causing the errors, disable and reenale the client (wireless NIC).</p>
CCMP Pkt Transfer Ct	Total number of CCMP packets sent and received by the radio.
Radio Recv Phy Err Ct	<p>Number of times radar caused packet errors. If this counter increments rapidly, there is a problem in the RF environment.</p> <p>Note: This counter increments only when radar is detected. Rate-specific Phy errors are instead counted in the PhyError columns for individual data rates.</p>

Table 36. Output for show ap counters

Field	Description
Radio Adjusted Tx Pwr	Current power level set on the radio. If RF Auto-Tuning of power is enabled, this value is the power set by RF Auto-Tuning. If RF Auto-Tuning is disabled, this value is the statically configured power level.
802.3 Packet Tx Ct	Number of raw 802.3 packets transmitted by the radio. These are LocalTalk (AppleTalk) frames. This counter increments only if LocalTalk traffic is present.
No Receive Descriptor	<p>Number of packets for which the UNIVERGE WL Access Points could not create a descriptor. A descriptor describes a received packet's size and its location in UNIVERGE WL Access Points memory. The UNIVERGE WL Access Points buffers descriptors, and clears them during interframe spaces.</p> <p>This counter increments if the UNIVERGE WL Access Points runs out of buffers for received packets. This condition can occur when a noise burst temporarily floods the air and the UNIVERGE WL Access Points attempts to buffer the noise as packets. Buffer overruns are normal while a UNIVERGE WL Access Point is booting. However, if they occur over an extended period of time when the UNIVERGE WL Access Points is fully active, this can indicate RF interference.</p>
Illegal Rates	Number of times a client attempted to connect with a disabled data rate.
PktTxCount	Number of packets transmitted by the radio.
MultiPktDrop	Number of multicast packets dropped by the radio due to a buffer overflow on the UNIVERGE WL Access Points. This counter increments if there is too much multicast traffic or there is a problem with the multicast packets. Normally, this counter should be 0.

Table 36. Output for show ap counters

Field	Description
MultiBytDrop	Number of multicast bytes dropped by the radio due to a buffer overflow on the UNIVERGE WL Access Points. (See the description for MultiPktDrop.)
User Sessions	<p>Number of clients currently associated with the radio.</p> <p>Generally, this counter is equal to the number of sessions listed for the radio in show sessions output. However, the counter can differ from the counter in show sessions output if a client is associated with the radio but has not yet completed 802.1X authentication. In this case, the client is counted by this counter but not in the show sessions output.</p> <p>Although there is no specific normal range for this counter, a high or low number relative to other radios can mean the radio is underutilized or overutilized relative to the other radios. (However, if the clients are VoIP phones, a relatively high number of clients does not necessarily mean overutilization since voice clients consume less bandwidth on average than data clients.)</p>
MIC Error Ct	<p>Number of times the radio received a TKIP-encrypted frame with an invalid MIC.</p> <p>Normally, the value of this counter should always be 0. If the value is not 0, check the system log for MIC error messages and contact UNIVERGE.</p>
TKIP Decrypt Err	<p>Number of times a decryption error occurred with a packet encrypted with TKIP.</p> <p>(See the description for CCMP Pkt Decrypt Err.)</p>
CCMP Pkt Replays	<p>Number of CCMP packets that were resent to the UNIVERGE WL Access Points by a client.</p> <p>(See the description for TKIP Pkt Replays.)</p>
RadioResets	Number of times the radio has been reset. Generally, a reset occurs as a result of RF noise. It is normal for this counter to increment a few times per day.

Table 36. Output for show ap counters

Field	Description
Transmit Retries	<p>Number of times the radio retransmitted a unicast packet because it was not acknowledged. The UNIVERGE WL Access Points uses this counter to adjust the transmit data rate for a client, in order to minimize retries.</p> <p>The ratio of transmit retries to transmitted packets (TxUniPkt) indicates the overall transmit quality. A ratio of about 1 retry to 10 transmitted packets indicates good transmit quality. A ratio of 3 or more to 10 indicates poor transmit quality.</p> <p>Note: This counter includes unacknowledged probes. Some clients do not respond to probes, which can make this counter artificially high.</p>
Noise Floor	<p>Received signal strength at which the UNIVERGE WL Access Points can no longer distinguish 802.11 packets from ambient RF noise. A value around -90 or higher is good for an 802.11b/g radio. A value around -80 or higher is good for an 802.11a radio. Values near 0 can indicate RF interference.</p>
802.3 Packet Rx Ct	<p>Number of raw 802.3 packets received by the radio. These are LocalTalk (AppleTalk) frames. This counter increments only if LocalTalk traffic is present.</p>
<p>The counters above are global for all data rates. The counters below are for individual data rates.</p> <p>Note: If counters for lower data rates are incrementing but counters for higher data rates are not incrementing, this can indicate poor throughput. The poor throughput can be caused by interference. If the cause is not interference or the interference cannot be eliminated, you might need to relocate the UNIVERGE WL Access Points in order to use the higher data rates and therefore improve throughput.</p>	
TxUniPkt	Number of unicast packets transmitted by the radio.
TxMultiPkt	Number of multicast packets transmitted by the radio.

Table 36. Output for show ap counters

Field	Description
TxUniByte	Number of unicast bytes transmitted by the radio.
TxMultiByte	Number of multicast bytes transmitted by the radio.
RxPkt	Number of packets received by the radio.
RxByte	Number of bytes received by the radio.
UndcrptPkt	Number of undecryptable packets received by the radio. It is normal for this counter to increment even in stable networks and does not necessarily indicate an attack. For example, a client might be sending incorrect key information. However, if the counter increments rapidly, there might be a problem in the network.
UndcrptByte	Number of undecryptable bytes received by the radio. (See the description for UndcrptPkt.)
PhyError	<p>Number of packets that could not be decoded by the UNIVERGE WL Access Points. This condition can have any of the following causes:</p> <ul style="list-style-type: none">• Collision of an 802.11 packet.• Packet whose source is too far away, thus rendering the packet unintelligible by the time it reaches the UNIVERGE WL Access Points.• Interference caused by an 802.11b/g phone or other source. <p>It is normal for this counter to be about 10 percent of the total RxByte count. It is also normal for higher data rates to have higher Phy error counts than lower data rates.</p>

See Also **show sessions network** on page 536

show ap fdb



Note. This command is not supported.

show ap qos-stats

Displays statistics for UNIVERGE WL Access Points forwarding queues.

Syntax `show ap qos-stats [ap-number] [clear]`

ap-number Index value that identifies the UNIVERGE WL Access Points on the UNIVERGE WL Controller.

clear Clears the counters after displaying their current values.

Defaults None.

Access Enabled.

Usage Repeating this command with the **clear** option at regular intervals allows you to monitor transmission and drop rates.

Examples The following command shows statistics for the UNIVERGE WL Access Points forwarding queues on a UNIVERGE WL Access Points:

```

PROPMT# show ap qos-stats 4
CoS   Queue      Tx           TxDrop
=====
    AP: 4 radio: 1
1,2   Background      0             0
0,3   BestEffort    15327         278
4,5   Video          0             0
6,7   Voice         1714881        0
    AP: 4 radio: 2
1,2   Background      0             0
0,3   BestEffort      0             0
4,5   Video           0             0
6,7   Voice           0             0

```

Table 37 describes the fields in this display.

Table 37. Output for show ap qos-stats

Field	Description
CoS	CoS value associated with the forwarding queues.
Queue	Forwarding queue.
AP	UNIVERGE WL Access Points number.
radio	Radio number.
Tx	Number of packets transmitted to the air from the queue.
TxDrop	Number of packets dropped from the queue instead of being transmitted. Some packet drops are normal, especially if the RF environment is <i>noisy</i> . Also, it is normal for a mildly congested radio to drop low-priority packets proportionally more often than high-priority packets. However, continuous packet drops from the Voice queue can indicate over-subscription or excessive interference in the RF environment.

show ap etherstats

Displays Ethernet statistics for an Ethernet port on a UNIVERGE WL Access Point.

Syntax `show ap etherstats ap-number`

ap-number Index value that identifies the UNIVERGE WL Access Points on the UNIVERGE WL Controller.

Defaults None.

Access Enabled.

Examples The following command displays Ethernet statistics for the Ethernet ports on UNIVERGE WL Access Points 1:

```

PROPMT# show ap etherstats 1
AP: 1 ether: 1
=====
RxUnicast:      75432 TxGoodFrames:      55210
RxMulticast:    18789 TxSingleColl:       32
RxBroadcast:     8 TxLateColl:           0
RxGoodFrames:   94229 TxMaxColl:         0
RxAlignErrs:     0 TxMultiColl:         47
RxShortFrames:  0 TxUnderruns:           0
RxCrcErrors:    0 TxCarrierLoss:         0
RxOverruns:     0 TxDeferred:          150
RxDiscards:     0
AP: 1 ether: 2
=====
RxUnicast:      64379 TxGoodFrames:      60621
RxMulticast:    21798 TxSingleColl:       32
RxBroadcast:    11 TxLateColl:           0
RxGoodFrames:   86188 TxMaxColl:         0
RxAlignErrs:     0 TxMultiColl:         12
RxShortFrames:  0 TxUnderruns:           0
RxCrcErrors:    0 TxCarrierLoss:         0
RxOverruns:     0 TxDeferred:          111
RxDiscards:     0

```

Table 38 describes the fields in this display.

Table 38. Output for show ap etherstats

Field	Description
RxUnicast	Number of unicast frames received.
RxMulticast	Number of multicast frames received.
RxBroadcast	Number of broadcast frames received.
RxGoodFrames	Number of frames received properly from the link.
RxAlignErrs	Number of received frames that were both misaligned and contained a CRC error.
RxShortFrames	Number of received frames that were shorter than the minimum frame length.
RxCrcErrors	Number of received frames that were discarded due to CRC errors.

Table 38. Output for show ap etherstats

Field	Description
RxOverruns	Number of frames known to be lost due to a temporary lack of hardware resources.
RxDiscards	Number of frames known to be lost due to a temporary lack of software resources.
TxGoodFrames	Number of frames transmitted properly on the link.
TxSingleColl	Number of transmitted frames that encountered a single collision.
TxLateColl	Number of frames that were not transmitted because they encountered a collision outside the normal collision window.
TxMaxColl	Number of frames that were not transmitted because they encountered the maximum allowed number of collisions. Typically, this occurs only during periods of heavy traffic on the network.
TxMultiColl	Number of transmitted frames that encountered more than one collision.
TxUnderruns	Number of frames that were not transmitted or retransmitted due to temporary lack of hardware resources.
TxCARRIERLoss	Number of frames transmitted despite the detection of a deassertion of CRS during the transmission.
TxDeferred	Number of frames deferred before transmission due to activity on the link.

show ap group

Displays configuration information and load-balancing status for AP groups.

Syntax `show ap group [name]`

name Name of an AP group.

Defaults None.

Access Enabled.

Examples The following command displays information for AP group *loadbalance1*:

PROMPT# `show ap group loadbalance1`

Load Balance Grp	Port	Clients	Status	Refused
loadbalance1	1	ap1	Accepting	0
loadbalance1	7	ap6	Refusing	2

Table 39 describes the fields in this display.

Table 39. Output for show ap group

Field	Description
Load Balance Grp	Name of the AP group.
Port	UNIVERGE WL Controller port number.
Clients	Number of active client sessions on the AP.

Table 39. Output for show ap group

Field	Description
Status	Association status of the AP: <ul style="list-style-type: none">• Accepting—The AP is accepting new associations.• Refusing—The AP is refusing new associations.
Refused	Number of association requests refused by the AP due to load balancing. UNIVERGE WL Control System resets this counter to 0 when the UNIVERGE WL Controller is restarted, UNIVERGE WL Control System is reloaded, or the AP is removed from the group.

See Also

- 1 **show ap config** on page 374

show ap status

Displays AP and radio status information.

Syntax **show ap status** [**terse**] | [*ap-number* | **all** [**radio** {**1** | **2**}]]

terse	Displays a brief line of essential status information for each UNIVERGE WL Access Points.
<i>ap-number</i>	Index value that identifies the UNIVERGE WL Access Points on the UNIVERGE WL Controller.
all	Shows status information for all directly attached UNIVERGE WL Access Points and all UNIVERGE WL Access Points configured on the UNIVERGE WL Controller.
radio 1	Shows status information for radio 1.
radio 2	Shows status information for radio 2. (This option does not apply to single-radio models.)

Defaults None.

Access Enabled.

Examples The following command displays the status of an AP:

```

PROPMT# show ap status 7
AP: 7, AP model: WL1500-AP, manufacturer NEC Infrontia, name: AP07
=====
State:      operational (not encrypt)
CPU info: Atheros:MIPS32 speed=2200000000 Hz version=AR5312, ram=16777216
          s/n=G8TZUB0028 hw_rev=B
Uptime:     503 hours, 51 minutes, 5 seconds

Radio 1 type: 802.11g, state: configure succeed [Enabled]
          operational channel: 11(Auto) operational power: 1
          bssid1: 00:60:b9:11:57:c0, ssid: public
          bssid2: 00:60:b9:11:57:c2, ssid: employee-net
          load balance: enabled, current load: (unavailable)
          RFID Reports: Inactive
Radio 2 type: 802.11a, state: configure succeed [Disabled](Sweep mode)
          operational channel: 44(Auto) operational power: 1
          bssid1: 00:60:b9:11:57:c1, ssid: mycorp-tkip
          load balance: enabled, current load: (unavailable)
          RFID Reports: Inactive

```

The following command uses the **terse** option to display brief information for UNIVERGE WL Access Points:

```

PROPMT# show ap status terse
Total number of entries: 120
Operational: 1, Image Downloading: 0, Unknown: 119, Other: 0
Flags: o = operational, b = booting, d = image downloading
       c = configuring, f = configuration failed
       a = auto AP, m = mesh AP, p = mesh portal
       i = insecure, e = encrypted, u = unencrypt
AP Flag IP Address   Model      MAC Address      Radio1 Radio2 Uptime
-----
7 o-u  10.8.255.11    WL1500-AP 00:60:b9:11:da:82 D11/1  D44/1  21d00h

```

Table 40 and Table 41 describe the fields in these displays.

Table 40. Output for show ap status

Field	Description
AP	Identifier for the UNIVERGE WL Access Points on the UNIVERGE WL Controller.
IP-addr	IP address of the UNIVERGE WL Access Points. The address is assigned to the UNIVERGE WL Access Points by a DHCP server. Note: This field is applicable only if the UNIVERGE WL Access Points is not directly attached to the UNIVERGE WL Controller.
AP model	AP model number.
manufacturer	Company that made the AP.
fingerprint	Hexadecimal fingerprint of the UNIVERGE WL Access Points public encryption key. Note: This field is displayed only if the UNIVERGE WL Access Points is not directly attached to the UNIVERGE WL Controller.
name	AP name.
Link	Status of this link with the AP at the other end of the link. The status can be up or down.

Table 40. Output for show ap status

Field	Description
State	<p>State of the AP:</p> <ul style="list-style-type: none"> • init—The AP has been recognized by the UNIVERGE WL Controller but has not yet begun booting. • booting—The AP has asked the UNIVERGE WL Controller for a boot image. • image downloading—The AP is receiving a boot image from the UNIVERGE WL Controller. • image downloaded—The AP has received a boot image from the UNIVERGE WL Controller and is booting. • configuring—The AP has booted and is ready to receive or is already receiving configuration parameters from the UNIVERGE WL Controller. • operational—The AP has received configuration parameters for one or more radios and is ready to accept client connections. • configure failure—One or more of the radio parameters received from the UNIVERGE WL Controller is invalid. <p>For UNIVERGE WL Access Points, this field also indicates whether the UNIVERGE WL Access Points management traffic with the UNIVERGE WL Controller is encrypted, and whether the UNIVERGE WL Access Points fingerprint has been verified on the UNIVERGE WL Controller:</p> <ul style="list-style-type: none"> • not encrypted—The management session is not encrypted. • encrypted but fingerprint not verified—The UNIVERGE WL Access Points management traffic is encrypted, but the UNIVERGE WL Access Points fingerprint has not been verified in UNIVERGE WL Control System.
State	<ul style="list-style-type: none"> • encrypted and verified—The UNIVERGE WL Access Points management traffic is encrypted and the UNIVERGE WL Access Points fingerprint has been verified in UNIVERGE WL Control System.

Table 40. Output for show ap status

Field	Description
CPU info	Specifications and identification of the CPU.
Uptime	Amount of time since the AP booted using this link.
Radio 1 type	802.11 type and configuration state of the radio.
Radio 2 type	<ul style="list-style-type: none"> • The <i>configure succeed</i> state indicates that the AP has received configuration parameters for the radio and the radio is ready to accept client connections. • <i>802.11b protect</i> indicates that the 802.11b/g radio is sending messages to 802.11b devices, while sending 802.11g traffic at higher data rates, to inform the 802.11b devices about the 802.11g traffic and reserve bandwidth for the traffic. Protection mode remains in effect until 60 seconds after the last 802.11b traffic is detected by the 802.11b/g radio. • <i>Sweep Mode</i> indicates that a disabled radio is nonetheless participating in rogue detection scans. Even though this message appears only for disabled radios, all radios, enabled or disabled, participate in rogue detection. • <i>Countermeasures Enabled</i> indicates that the radio is sending countermeasures packets to combat a rogue. • <i>Radar Scan</i> indicates that the radio is performing the initial channel availability check for Dynamic Frequency Selection (DFS). This state lasts during the first 60 seconds an 802.11a radio is on a new channel, during which time the radio does not transmit. If the radio does not detect any radar on the channel, the radio starts using the channel for data. If the radio does detect radar, the flag changes to <i>Radar Detected</i>. (See below).

Table 40. Output for show ap status

Field	Description
Radio 1 type Radio 2 type (cont.)	<ul style="list-style-type: none"> <i>Radar Detected</i> indicates that DFS has detected radar on the channel. When this occurs, the UNIVERGE WL Access Points stops transmitting on the channel for 30 minutes. If RF Auto-Tuning is enabled for channel assignment, the radio selects another channel and performs the initial channel availability check on the new channel, during which time the flag changes back to <i>Radar Scan</i>. <p>Note: <i>Radar Scan</i> and <i>Radar Detected</i> apply only to 802.11a radios, for country codes that use DFS.</p> <ul style="list-style-type: none"> The following information appears for external antennas: <ul style="list-style-type: none"> <i>External antenna detected, configured as antenna-model</i>—Indicates that an external antenna has been detected, and lists the antenna model configured on the radio. (UNIVERGE WL Control System does not detect the specific model.) <i>External antenna detected, not configured</i>—Indicates that an external antenna was detected but no external antenna is configured on the radio. <i>External antenna not detected, configured as antenna-model</i>—Indicates that an external antenna is configured on the radio but no external antenna was detected.
operational channel	<p>The channel on which the radio is currently operating.</p> <p>Note: If the channel number is followed by <i>(Auto)</i>, the value was set by RF Auto-Tuning.</p>
operational power	<p>The power level at which the radio is currently operating.</p> <p>Note: If the power setting is followed by <i>(Auto)</i>, the value was set by RF Auto-Tuning.</p>

Table 40. Output for show ap status

Field	Description
bssid, ssid	SSIDs configured on the radio and their BSSIDs.
load balance	Whether RF load balancing is enabled for the radio
current load	The load on this radio relative to the load balancing group average or target load.
RFID Reports	<p>Status of AeroScout asset tag support.</p> <ul style="list-style-type: none"> Active—The AeroScout Engine has enabled the tag report mode on the UNIVERGE WL Access Points. Inactive—The AeroScout Engine has not enabled, or has disabled, the tag report mode on the UNIVERGE WL Access Points. <p>Note: This field is displayed only if the rfid-mode option is enabled on the radio profile that manages the radio.</p>

Table 41. Output for show ap status terse

Field	Description
AP	The number of the UNIVERGE WL Access Points connected.
Flag	<p>Operational status flags for the UNIVERGE WL Access Points.</p> <p>For flag definitions, see the key in the command output.</p>
IP Address	<p>IP address of the UNIVERGE WL Access Points. The address is assigned to the UNIVERGE WL Access Points by a DHCP server.</p> <p>Note: This field is applicable only if the UNIVERGE WL Access Points is configured on the UNIVERGE WL Controller as a UNIVERGE WL Access Points.</p>
Model	AP model number.

Table 41. Output for show ap status terse

Field	Description
MAC Address	MAC address of the UNIVERGE WL Access Points.
Radio1	State, channel, and power information for radio 1: <ul style="list-style-type: none">• The state can be D (disabled) or E (enabled).• The channel and power settings are shown as <i>channel/power</i>.
Radio2	State, channel, and power information for radio 2.
Uptime	Amount of time since the AP booted using this link.

show ap vlan



Note. This command is not supported.

show auto-tune attributes

Displays the current values of the RF attributes RF Auto-Tuning uses to decide whether to change channel or power settings.

Syntax **show auto-tune attributes**
[ap ap-number [radio {1 | 2 | all}]]

<i>ap-number</i>	Index value that identifies the UNIVERGE WL Access Points on the UNIVERGE WL Controller.
radio 1	Shows RF attribute information for radio 1.
radio 2	Shows RF attribute information for radio 2. (This option does not apply to single-radio models.)
radio all	Shows RF attribute information for both radios.

Defaults None.

show auto-tune attributes

Chapter 12

Access Enabled.

Examples The following command displays RF attribute information for radio 1 on the connected UNIVERGE WL Access Points 2:

```
PROPMT# show auto-tune attributes ap 2 radio 1
Auto-tune attributes for ap 2 radio 1:
Noise: -92 Packet Retransmission Count: 0
Utilization: 0 Phy Errors Count: 0
CRC Errors count: 122
```

Table 42 describes the fields in this display.

Table 42. Output for show auto-tune attributes

Field	Description
Noise	Noise threshold on the active channel. RF Auto-Tuning prefers channels with low noise levels over channels with higher noise levels.
Utilization	Number of multicast packets per second that a radio can send on a channel while continuously sending fixed size frames over a period of time. The number of packets that are successfully transmitted indicates how busy the channel is.
CRC Errors count	Number of frames received by the radio on that active channel that had CRC errors. A high CRC error count can indicate a hidden node or co-channel interference.
Packet Retransmission Count	Number of retransmitted packets sent from the client to the radio on the active channel. Retransmissions can indicate that the client is not receiving ACKs from the UNIVERGE WL Access Points radio.
Phy Errors Count	Number of frames received by the UNIVERGE WL Access Points radio that had physical layer errors on the active channel. Phy errors can indicate interference from a non-802.11 device.

See Also

- 1 **set ap radio auto-tune max-power** on page 292

- 1 **set radio-profile auto-tune channel-config** on page 301
- 1 **set radio-profile auto-tune channel-holddown** on page 303
- 1 **set radio-profile auto-tune channel-interval** on page 304
- 1 **set radio-profile auto-tune power-config** on page 305
- 1 **set radio-profile auto-tune power-interval** on page 306
- 1 **show auto-tune neighbors** on page 399
- 1 **show radio-profile** on page 408

show auto-tune neighbors

Displays the other AP radios and third-party 802.11 radios that an AP radio can hear.

Syntax **show auto-tune neighbors**
[**ap** *ap-number* [**radio** {**1** | **2** | **all**}]]

<i>ap-number</i>	Index value that identifies the UNIVERGE WL Access Points on the UNIVERGE WL Controller.
radio 1	Shows neighbor information for radio 1.
radio 2	Shows neighbor information for radio 2. (This option does not apply to single-radio models.)
radio all	Shows neighbor information for both radios.

Defaults None.

Access Enabled.

Usage For simplicity, this command displays a single entry for each AP radio, even if the radio is supporting multiple BSSIDs. However, BSSIDs for third-party 802.11 radios are listed separately, even if a radio is supporting more than one BSSID.

show auto-tune neighbors

Chapter 12

Information is displayed for a radio if the radio sends beacon frames or responds to probe requests. Even if the radio SSIDs are unadvertised, AP radios detect the empty beacon frames (beacon frames without SSIDs) sent by the radio, and include the radio in the neighbor list.

Examples The following command displays neighbor information for radio 1 on the connected AP 2:

```
PROPMTH# show auto-tune neighbors ap 2 radio 1
Total number of entries for ap 2 radio 1: 5
Channel Neighbor BSS/MAC  RSSI
-----
1 00:60:b9:11:e3:60  -46
1 00:60:b9:11:0a:80  -78
1 00:60:b9:11:d2:c0  -74
1 00:60:b9:11:dd:00  -50
1 00:60:b9:11:05:c1  -72
```

Table 43 describes the fields in this display.

Table 43. Output for show auto-tune neighbors

Field	Description
Channel	Channel on which the BSSID is detected.
Neighbor BSS/MAC	BSSID detected by the radio.
RSSI	Received signal strength indication (RSSI), in decibels referred to 1 milliwatt (dBm). A higher value indicates a stronger signal.

See Also

- 1 **set ap radio auto-tune max-power** on page 292
- 1 **set radio-profile auto-tune channel-config** on page 301
- 1 **set radio-profile auto-tune channel-holddown** on page 303
- 1 **set radio-profile auto-tune channel-interval** on page 304
- 1 **set radio-profile auto-tune power-config** on page 305
- 1 **set radio-profile auto-tune power-interval** on page 306

1 **show auto-tune attributes** on page 397

1 **show radio-profile** on page 408

show ap boot-configuration

Displays information about the static IP address configuration (if any) on a UNIVERGE WL Access Points.

Syntax **show ap boot-configuration** *ap-number*

ap-number Index value that identifies the UNIVERGE WL Access Points on the UNIVERGE WL Controller.

Defaults None.

Access Enabled.

Examples The following command displays static IP configuration information for UNIVERGE WL Access Points 1:

```
PROPMT# show ap boot-configuration 1
```

```
Static Boot Configuration
AP: 7
```

```
IP Address: Disabled
VLAN Tag: Disabled
Switch: Disabled
```

```
Mesh: Disabled
```

```
IP Address:
Netmask:
Gateway:
VLAN Tag:
Switch IP:
Switch Name:
DNS IP:
Mesh SSID:
Mesh PSK:
```

Table 44 describes the fields in this display.

Table 44. Output for show ap boot-configuration

Field	Description
AP	UNIVERGE WL Access Points number.
IP Address	Whether static IP address assignment is enabled for this UNIVERGE WL Access Points.
VLAN Tag	Whether the UNIVERGE WL Access Points is configured to use a VLAN tag.
Switch	Whether the UNIVERGE WL Access Points is configured to use a manually specified UNIVERGE WL Controller as its boot device.
Mesh	Whether WLAN mesh services are enabled for this UNIVERGE WL Access Points.
IP Address	The static IP address assigned to this UNIVERGE WL Access Points.
Netmask	The subnet mask assigned to this UNIVERGE WL Access Points.
Gateway	The IP address of the default gateway assigned to this UNIVERGE WL Access Points.
Vlan Tag	The VLAN tag that the UNIVERGE WL Access Points is configured to use (if any).
Switch IP	The IP address of the UNIVERGE WL Controller that this UNIVERGE WL Access Points is configured to use as its boot device (if any).
Switch Name	The Switch Name of the UNIVERGE WL Controller that this UNIVERGE WL Access Points is configured to use as its boot device (if any).
DNS IP	The IP address of the DNS server that the UNIVERGE WL Access Points uses to resolve the name of the UNIVERGE WL Controller used as its boot device.

Table 44. Output for show ap boot-configuration

Field	Description
Mesh SSID	The WLAN mesh services SSID this UNIVERGE WL Access Points is configured to use (if any)
Mesh PSK	The preshared key (PSK) the UNIVERGE WL Access Points uses for authentication with a Mesh Portal AP (if any).

show ap connection

Displays the system IP address of the UNIVERGE WL Controller that booted a UNIVERGE WL Access Points.

Syntax `show ap connection` [*ap-number* | **serial-id** *serial-ID*]

ap-number Index value that identifies the UNIVERGE WL Access Points on the UNIVERGE WL Controller.

serial-id *serial-ID* AP serial ID.

Defaults None.

Access Enabled.

Usage The **serial-id** parameter displays the active connection for the specified UNIVERGE WL Access Points even if that UNIVERGE WL Access Points is not configured on this UNIVERGE WL Controller. If you instead use the command with the *ap-number* parameter or without a parameter, connection information is displayed only for UNIVERGE WL Access Points that are configured on this UNIVERGE WL Controller.

This command provides information only if the UNIVERGE WL Access Points is configured on the UNIVERGE WL Controller where you use the command. The UNIVERGE WL Controller does not need to be the one that booted the UNIVERGE WL Access Points, but it must have the UNIVERGE WL Access Points in its configuration. Also, the UNIVERGE WL Controller that booted the UNIVERGE WL Access Points must be in the same Mobility Domain as the UNIVERGE WL Controller where you use the command.

show ap connection

Chapter 12

If a UNIVERGE WL Access Points is configured on this UNIVERGE WL Controller (or another UNIVERGE WL Controller in the same Mobility Domain) but does not have an active connection, the command does not display information for the UNIVERGE WL Access Points. To show connection information for UNIVERGE WL Access Points, use the **show ap global** command on one of the UNIVERGE WL Controllers where the UNIVERGE WL Access Points are configured.

Examples The following command displays information for all UNIVERGE WL Access Points configured on this UNIVERGE WL Controller that have active connections:

```
PROPMT# show ap connection
Total number of entries: 1
AP  Serial Id  AP IP Address  Switch IP Address
---
3   G8TZUB0028  192.168.1.52   192.168.10.20
```

The following command displays connection information specifically for a UNIVERGE WL Access Point with serial ID *G8TZUB0028*:

```
PROPMT# show ap connection serial-id G8TZUB0028
Total number of entries: 1
AP  Serial Id  AP IP Address  Switch IP Address
---
3   G8TZUB0028  192.168.1.52   192.168.10.20
```

Table 45 describes the fields in this display.

Table 45. Output for show ap connection

Field	Description
AP	ID assigned to the UNIVERGE WL Access Point. If the connection is configured on another UNIVERGE WL Controller, this field contains a hyphen (-).
Serial Id	Serial ID of the AP.

Table 45. Output for show ap connection

Field	Description
AP IP Address	IP address assigned by DHCP to the UNIVERGE WL Access Point.
Switch IP Address	System IP address of the UNIVERGE WL Controller on which the UNIVERGE WL Access Point has an active connection. This is the UNIVERGE WL Controller that the UNIVERGE WL Access Point used for booting and configuration and is using for data transfer.

See Also

- 1 **show ap config** on page 374
- 1 **show ap global** on page 405
- 1 **show ap unconfigured** on page 407

show ap global

Displays connection information for UNIVERGE WL Access Points configured on a UNIVERGE WL Controller .

Syntax **show ap global** [*ap-number* | **serial-id** *serial-ID*]

ap-number Index value that identifies the UNIVERGE WL Access Points on the UNIVERGE WL Controller.

serial-id *serial-ID* AP serial ID.

Defaults None.

Access Enabled.

Usage Connections are shown only for the UNIVERGE WL Access Points that are configured on the UNIVERGE WL Controller from which you enter the command, and only for the Mobility Domain the UNIVERGE WL Controller is in.

show ap global

Chapter 12

To show information only for UNIVERGE WL Access Points that have active connections, use the **show ap connection** command.

Examples The following command displays connection information for all the UNIVERGE WL Access Points configured on a UNIVERGE WL Controller:

```
PROPMT# show ap global
AP  Serial Id  Switch IP Address
---
3   G8TZUB0053 192.168.10.10  HIGH
4   G8TZUB0253 192.168.10.20  LOW
```

Table 46 describes the fields in this display.

Table 46. Output for show ap global

Field	Description
AP	ID you assigned to the UNIVERGE WL Access Point. Note: AP numbers are listed only for UNIVERGE WL Access Points configured on this UNIVERGE WL Controller. If the field contains a hyphen (-), the UNIVERGE WL Access Point configuration displayed in the row of output is on another UNIVERGE WL Controller.
Serial Id	Serial ID of the UNIVERGE WL Access Points.
Switch IP Address	System IP address of the UNIVERGE WL Controller on which the UNIVERGE WL Access Points is configured. A separate row of output is displayed for each UNIVERGE WL Controller on which the UNIVERGE WL Access Points is configured.
Bias	Bias of the UNIVERGE WL Controller for the UNIVERGE WL Access Points: <ul style="list-style-type: none">• High• Low

See Also

- 1 **set ap** on page 54
- 1 **set ap bias** on page 282
- 1 **show ap config** on page 374
- 1 **show ap connection** on page 403
- 1 **show ap unconfigured** on page 407

show ap unconfigured

Displays UNIVERGE WL Access Points that are physically connected to the network but that are not configured on any UNIVERGE WL Controllers.

Syntax **show ap unconfigured**

Defaults None.

Access Enabled.

Usage If a UNIVERGE WL Access Points is configured on a UNIVERGE WL Controller in another Mobility Domain, the UNIVERGE WL Access Points can appear in the output until the UNIVERGE WL Access Points is able to establish a connection with a UNIVERGE WL Controller in its Mobility Domain. After the UNIVERGE WL Access Points establishes a connection, the entry for the UNIVERGE WL Access Points ages out and no longer appears in the command output.

Entries in the command output table age out after two minutes.

Examples The following command displays information for two UNIVERGE WL Access Points that are not configured:

```
PROPMT# show ap unconfigured
Serial Id: g8tzub0053 Model: WL1500-AP IP Address: 172.16.221.21
Port: 1 Vlan: default
```

Table 47 describes the fields in this display.

Table 47. Output for show ap unconfigured

Field	Description
Serial Id	Serial ID of the UNIVERGE WL Access Points.
Model	UNIVERGE WL Access Points model number.
IP Address	IP address of the UNIVERGE WL Access Points. This is the address that the UNIVERGE WL Access Points receives from a DHCP server. The UNIVERGE WL Access Points uses this address to send a Find UNIVERGE WL Controller message to request configuration information from UNIVERGE WL Controllers. However, the UNIVERGE WL Access Points cannot use the address to establish a connection unless the UNIVERGE WL Access Points first receives a configuration from a UNIVERGE WL Controller.
Port	Port number on which this UNIVERGE WL Controller received the UNIVERGE WL Access Points Find UNIVERGE WL Controller message.
VLAN	VLAN on which this UNIVERGE WL Controller received the UNIVERGE WL Access Points Find UNIVERGE WL Controller message.

See Also

- 1 **show ap connection** on page 403
- 1 **show ap global** on page 405

show radio-profile

Displays radio profile information.

Syntax `show radio-profile {name | ?}`

name Displays information about the named radio profile.

`?` Displays a list of radio profiles.

Defaults None.

Access Enabled.

Usage UNIVERGE WL Control System contains a *default* radio profile. UNIVERGE WL Control System recommends that you do not change this profile but instead keep the profile for reference.

Examples The following command shows radio profile information for the *default* radio profile:

```

PROPMTH# show radio-profile default
Beacon Interval:          100    DTIM Interval:          1
Max Tx Lifetime:         2000    Max Rx Lifetime:         2000
RTS Threshold:           2346    Frag Threshold:          2346
Long Preamble:           no      Tune Channel:            yes
Tune Power:              no      Tune Channel Interval:    3600
Tune Power Interval:     600     Power ramp interval:      60
Channel Holddown:        300     Countermeasures:          none
Active-Scan:             yes     RFID enabled:             no
WMM Powersave:          no      QoS Mode:                 wmm

Service profiles: sp1*

```

Table 48 describes the fields in this display.

Table 48. Output for show radio-profile

Field	Description
Beacon Interval	Rate (in milliseconds) at which each AP radio in the profile advertises the beacons SSID.
DTIM Interval	Number of times after every beacon that each AP radio in the radio profile sends a delivery traffic indication map (DTIM).
Max Tx Lifetime	Number of milliseconds that a frame <i>received</i> by a radio in the radio profile can remain in buffer memory.

Table 48. Output for show radio-profile

Field	Description
Max Rx Lifetime	Number of milliseconds that a frame <i>scheduled to be transmitted</i> by a radio in the radio profile can remain in buffer memory.
RTS Threshold	Minimum length (in bytes) a frame can be for a radio in the radio profile to use the RTS/CTS method to send the frame. The RTS/CTS method clears the air of other traffic to avoid corruption of the frame due to a collision with another frame.
Frag Threshold	Maximum length (in bytes) a frame is allowed to be without being fragmented into multiple frames before transmission by a radio in the radio profile.
Long Preamble	Indicates whether an 802.11b radio that uses this radio profile advertises support for frames with long preambles only: <ul style="list-style-type: none">• YES—Advertises support for long preambles only.• NO—Advertises support for long and short preambles.
Tune Channel	Indicates whether RF Auto-Tuning is enabled for dynamically setting and tuning channels.
Tune Power	Indicates whether RF Auto-Tuning is enabled for dynamically setting and tuning power levels.
Tune Channel Interval	Interval, in seconds, at which RF Auto-Tuning decides whether to change the channels on radios in a radio profile. At the end of each interval, UNIVERGE WL Control System processes the results of the RF scans performed during the previous interval, and changes radio channels if needed.

Table 48. Output for show radio-profile

Field	Description
Tune Power Interval	Interval, in seconds, at which RF Auto-Tuning decides whether to change the power level on radios in a radio profile. At the end of each interval, UNIVERGE WL Control System processes the results of the RF scans performed during the previous interval, and changes radio power levels if needed.
Power ramp interval	Number of seconds a radio waits before increasing or decreasing its power by 1 dBm in response to a power change from RF Auto-Tuning. After each power ramp interval, the radio increases or decreases the power by another 1 dB until the radio reaches the power level selected by RF Auto-Tuning.
Channel Holddown	Minimum number of seconds a radio in a radio profile must remain at its current channel assignment before RF Auto-Tuning can change the channel.
Countermeasures	Indicates whether countermeasures are enabled.
Active-Scan	Indicates whether the active-scan mode of RF detection is enabled.
RFID enabled	Indicates whether AeroScout tag support is enabled.
WMM Powersave	Indicates whether U-APSD support is enabled.

Table 48. Output for show radio-profile

Field	Description
QoS Mode	<p>Indicates the Quality-of-Service setting for UNIVERGE WL Access Points radio forwarding queues:</p> <ul style="list-style-type: none"> • voice-ext—Priority treatment is provided to voice traffic for NEC handsets. • svp—UNIVERGE WL Access Points forwarding queues are optimized for SpectraLink Voice Priority (SVP). • wmm—UNIVERGE WL Access Points forwarding queues provide standard priority handling for WMM devices. Traffic is classified and marked based on 802.1p and DSCP values. <p>For information about the QoS modes, see the “Configuring Quality of Service” chapter in the Configuration Guide.</p>
Service profiles	<p>Service profiles mapped to this radio profile. Each service profile contains an SSID and encryption information for that SSID.</p> <p>Note: An asterisk (*) next to the service profile name indicates that the CAC mode of the service profile is set to voice-ext. For a radio to provide bandwidth-based voice service to clients, the QoS mode of the radio profile must be voice-ext and the CAC mode of the service profile mapped to the radio profile must also be voice-ext.</p>

See Also

- 1 **set radio-profile active-scan** on page 300
- 1 **set radio-profile auto-tune channel-config** on page 301
- 1 **set radio-profile auto-tune channel-holddown** on page 303
- 1 **set radio-profile auto-tune channel-interval** on page 304
- 1 **set radio-profile auto-tune power-config** on page 305

- 1 **set radio-profile auto-tune power-interval** on page 306
- 1 **set radio-profile beacon-interval** on page 307
- 1 **set radio-profile countermeasures** on page 307
- 1 **set radio-profile dtim-interval** on page 309
- 1 **set radio-profile frag-threshold** on page 310
- 1 **set radio-profile max-rx-lifetime** on page 311
- 1 **set radio-profile max-tx-lifetime** on page 312
- 1 **set radio-profile mode** on page 316
- 1 **set radio-profile preamble-length** on page 320
- 1 **set radio-profile qos-mode** on page 321
- 1 **set radio-profile rts-threshold** on page 323
- 1 **set radio-profile service-profile** on page 324

show service-profile

Displays service profile information.

Syntax **show service-profile** {*name* | ?}

name Displays information about the named service profile.

? Displays a list of service profiles.

Defaults None.

Access Enabled.

Examples The following command displays information for service profile *sp1*:

```

PROPMT# show service-profile sp1
ssid-name:                dangssid  ssid-type:                crypto
Beacon:                   yes       Proxy ARP:                yes
DHCP restrict:            no       No broadcast:             no
Short retry limit:        3         Long retry limit:         3
Auth fallthru:            none     Sygate On-Demand (SODA):  no

```

show service-profile

Chapter 12

```
Enforce SODA checks:          yes   SODA remediation ACL:
Custom success web-page:      Custom failure web-page:
Custom logout web-page:      Custom agent-directory:
Static COS:                   no     COS: 0
Client DSCP:                  no     CAC mode: voice-ext
CAC sessions:                 12     User idle timeout: 180
Idle client probing:          yes    Keep initial vlan: no
Web Portal Session Timeout:   5     Mesh enabled: no
Web Portal ACL:               Bridging enabled: no
Load Balance Exempt:          no     Web Portal Logout: no
Custom Web Portal Logout URL:
WEP Key 1 value:              <none> WEP Key 2 value:      <none>
WEP Key 3 value:              <none> WEP Key 4 value:      <none>
WEP Unicast Index:            1     WEP Multicast Index: 1
Shared Key Auth:              NO
11a beacon rate:              6.0   multicast rate:      AUTO
11a mandatory rate: 6.0,12.0,24.0 standard rates: 9.0,18.0,36.0,48.0,54.0
11b beacon rate:              5.5   multicast rate:      AUTO
11b mandatory rate: 5.5,11.0 standard rates: 1.0,2.0
11g beacon rate:              5.5   multicast rate:      AUTO
11g mandatory rate: 1.0,2.0,5.5,11.0,6.0,12.0 standard rates: 9.0,18.0,24.0,
36.0,48.0,54.0
```

Table 49 describes the fields in this display.

Table 49. Output for show service-profile

Field	Description
ssid-name	Service set identifier (SSID) managed by this service profile.
ssid-type	SSID type: <ul style="list-style-type: none">• crypto—Wireless traffic for the SSID is encrypted.• clear—Wireless traffic for the SSID is unencrypted.
Beacon	Indicates whether the radio sends beacons, to advertise the SSID: <ul style="list-style-type: none">• no• yes
Proxy ARP	Indicates whether proxy ARP is enabled. When this feature is enabled, UNIVERGE WL Control System answers ARP requests on behalf of wireless clients.

Table 49. Output for show service-profile

Field	Description
DHCP restrict	Indicates whether DHCP Restrict is enabled. When this feature is enabled, UNIVERGE WL Control System allows only DHCP traffic for a new client until the client has successfully completed authentication and authorization.
No broadcast	Indicates whether broadcast restriction is enabled. When this feature is enabled, UNIVERGE WL Control System sends ARP requests and DHCP Offers and Acks as unicasts to their target clients instead of forwarding them as broadcasts.
Short retry limit	Number of times a radio serving the service-profile's SSID can send a short unicast frame without receiving an acknowledgment.
Long retry limit	Number of times a radio serving the service-profile's SSID can send a long unicast frame without receiving an acknowledgment. A long unicast frame is a frame that is <i>equal to or longer than</i> the RTS threshold.
Auth fallthru	<p>Secondary (fallthru) encryption type when a user tries to authenticate but the UNIVERGE WL Controller managing the radio does not have an authentication rule with a userglob that matches the username.</p> <ul style="list-style-type: none"> last-resort—Automatically authenticates the user and allows access to the SSID requested by the user, without requiring a username and password. none—Denies authentication and prohibits the user from accessing the SSID. web-portal—Redirects the user to a web page for login to the SSID.
Sygate On-Demand (SODA)	Whether SODA functionality is enabled for the service profile. When SODA functionality is enabled, connecting clients download SODA agent files, which perform security checks on the client.

Table 49. Output for show service-profile

Field	Description
Enforce SODA checks	Whether a client is allowed access to the network after it has downloaded and run the SODA agent security checks. When SODA functionality is enabled, and the UNIVERGE WL Controller is configured to enforce SODA checks, then a connecting client must download the SODA agent files and pass the checks in order to gain access to the network.
SODA remediation ACL	The name of the ACL to be applied to the client if it fails the SODA agent checks. If no remediation ACL is specified, then a client is disconnected from the network if it fails the SODA agent checks.
Custom success web-page	The name of the user-specified page that the client loads upon successful completion of the SODA agent checks. If no page is specified, then the success page is generated dynamically.
Custom failure web-page	The name of the user-specified page that the client loads if it fails SODA agent checks. If no page is specified, then the failure page is generated dynamically.
Custom logout web-page	The name of the user-specified page that the client loads upon logging out of the network, either by closing the SODA virtual desktop, or by requesting the page. If no page is specified, then the client is disconnected without loading a logout page.
Custom agent-directory	The name of the directory for SODA agent files on the UNIVERGE WL Controller, if different from the default. By default, SODA agent files are stored in a directory with the same name as the service profile.
Static COS	Indicates whether static CoS assignment is enabled. When this feature is enabled, UNIVERGE WL Access Points assign the CoS value in the COS field to all user traffic forwarded by the UNIVERGE WL Access Points.

Table 49. Output for show service-profile

Field	Description
COS	CoS value assigned by the UNIVERGE WL Access Points to all user traffic, if static CoS is enabled. (If static CoS is disabled, WMM or ACLs are used to assign CoS.)
Client DSCP	Whether packets are classified based on client DSCP level instead of 802.11 priority.
CAC mode	Call Admission Control mode: <ul style="list-style-type: none"> • none—CAC is disabled. • session—CAC is based on the number of active user sessions. If a UNIVERGE WL Access Point radio reaches the maximum number of active user sessions specified in the CAC session field, the UNIVERGE WL Access Points radio rejects new connection attempts.
CAC sessions	Maximum number of user sessions that can be active on a UNIVERGE WL Access Point radio at one time, if the CAC mode is session. Note: This value applies only when the CAC mode is session .
User idle timeout	Indicates how many seconds a user session can remain idle (indicated by no user traffic and no reply to client keepalive probes) before the session is changed to the Disassociated state.
Idle client probing	Indicates whether client keepalive probes are enabled.
Keep initial VLAN	Indicates whether the keep-initial-vlan option is enabled.
Web Portal Session Timeout	When a Web Portal Web Authentication session is placed in the Deassociated state, how many seconds the session can remain in that state before being terminated automatically.
Mesh enabled	Whether WLAN mesh services are enabled for the service profile.

Table 49. Output for show service-profile

Field	Description
Web Portal ACL	Name of the ACL used to filter traffic for Web Portal users associated with this service profile's SSID while the users are being authenticated.
Bridging enabled	Whether wireless bridging is enabled for this service profile.
Load Balance Exempt	Whether the UNIVERGE WL Access Points radios managed by this service profile are exempted (do not participate in) RF load balancing.
Web Portal Logout	Whether the Web Portal WebAAA logout functionality has been enabled.
Custom Web Portal Logout URL	If configured, the URL that Web Portal WebAAA users can access in order to terminate their sessions.
WEP Key 1 value	<p>State of static WEP key number 1. Radios can use this key to encrypt traffic with static Wired-Equivalent Privacy (WEP):</p> <ul style="list-style-type: none"> • none—The key is not configured. • preset—The key is configured. <p>Note: The WEP parameters apply to traffic only on the encrypted SSID.</p>
WEP Key 2 value	<p>State of static WEP key number 2:</p> <ul style="list-style-type: none"> • none—The key is not configured. • preset—The key is configured.
WEP Key 3 value	<p>State of static WEP key number 3:</p> <ul style="list-style-type: none"> • none—The key is not configured. • preset—The key is configured.
WEP Key 4 value	<p>State of static WEP key number 4:</p> <ul style="list-style-type: none"> • none—The key is not configured. • preset—The key is configured.
WEP Unicast Index	Index of the static WEP key used to encrypt unicast traffic on an encrypted SSID.

Table 49. Output for show service-profile

Field	Description
WEP Multicast Index	Index of the static WEP key used to encrypt multicast traffic on an encrypted SSID.
Shared Key Auth	Indicates whether shared-key authentication is enabled.
WPA enabled or RSN enabled	<p>Indicates that the Wi-Fi Protected Access (WPA) or Robust Security Network (RSN) information element (IE) is enabled. Additional fields display the settings of other WPA or RSN parameters:</p> <ul style="list-style-type: none"> • ciphers—Lists the cipher suites advertised by radios in the radio profile mapped to this service profile. • authentication—Lists the authentication methods supported for WPA or RSN clients: <ul style="list-style-type: none"> • 802.1X—dynamic authentication • PSK—preshared key authentication • TKIP countermeasures time—Indicates the amount of time (in ms) UNIVERGE WL Control System enforces countermeasures following a second message integrity code (MIC) failure within a 60-second period. <p>Note: These fields are displayed only when the WPA IE or RSN IE is enabled.</p>
vlan-name, session-timeout, service-type	<p>These are examples of authorization attributes that are applied by default to a user accessing the SSID managed by this service profile (in addition to any attributes assigned to the user by a RADIUS server or the local database).</p> <p>Attributes are listed here only if they have been configured as default attribute settings for the service profile.</p> <p>See Table 25 on page 223 for a list of authorization attributes and values that can be assigned to network users.</p>

Table 49. Output for show service-profile

Field	Description
11a / 11b / 11g transmit rate fields	<p>Data transmission rate settings for each radio type:</p> <ul style="list-style-type: none"> • beacon rate—Data rate of beacon frames sent by UNIVERGE WL Access Points radios. • multicast rate—Data rate of multicast frames sent by UNIVERGE WL Access Points radios. If the rate is auto, the UNIVERGE WL Access Points sets the multicast rate to the highest rate that can reach all clients connected to the radio. • mandatory rates—Set of data transmission rates that clients are required to support in order to associate with an SSID on a UNIVERGE WL Access Point radio. A client must support at least one of the mandatory rates. • standard rates—The set of valid rates that are neither mandatory nor disabled. These rates are supported for data transmission from the UNIVERGE WL Access Points radios. • disabled rates—Data transmission rates that UNIVERGE WL Access Points radios will not use to transmit data. (The radios will still accept frames from clients at disabled data rates.)

See Also

- 1 **set service-profile attr** on page 334
- 1 **set service-profile auth-dot1x** on page 336
- 1 **set service-profile auth-fallthru** on page 337
- 1 **set service-profile auth-psk** on page 339
- 1 **set service-profile beacon** on page 340
- 1 **set service-profile cac-mode** on page 341
- 1 **set service-profile cac-session** on page 342
- 1 **set service-profile cipher-ccmp** on page 343
- 1 **set service-profile cipher-tkip** on page 343

- 1 **set service-profile cipher-wep104** on page 344
- 1 **set service-profile cipher-wep40** on page 346
- 1 **set service-profile cos** on page 347
- 1 **set service-profile dhcp-restrict** on page 348
- 1 **set service-profile idle-client-probing** on page 349
- 1 **set service-profile long-retry-count** on page 351
- 1 **set service-profile no-broadcast** on page 351
- 1 **set service-profile proxy-arp** on page 353
- 1 **set service-profile psk-phrase** on page 354
- 1 **set service-profile psk-raw** on page 355
- 1 **set service-profile rsn-ie** on page 356
- 1 **set service-profile shared-key-auth** on page 357
- 1 **set service-profile short-retry-count** on page 358
- 1 **set service-profile ssid-name** on page 359
- 1 **set service-profile ssid-type** on page 359
- 1 **set service-profile static-cos** on page 360
- 1 **set service-profile tkip-mc-time** on page 361
- 1 **set service-profile transmit-rates** on page 362
- 1 **set service-profile user-idle-timeout** on page 365
- 1 **set service-profile web-portal-form** on page 366
- 1 **set service-profile web-portal-session-timeout** on page 368
- 1 **set service-profile wep active-multicast-index** on page 369
- 1 **set service-profile wep active-unicast-index** on page 370
- 1 **set service-profile wep key-index** on page 371
- 1 **set service-profile wpa-ie** on page 372

show service-profile cac session

Displays current session counts on all UNIVERGE WL Access Points using the specified service profile, when session-based CAC is enabled.

Syntax **show service-profile** *name* **cac session**

name Displays information about the named service profile.

Defaults None.

Access Enabled.

Examples The following command displays information about session counts for service profile *sp1*:

```
PROMPT# show service-profile sp1 cac session
Service Profile sp1
CAC Mode          SESSION
Max Sessions      14
```

Table 50 describes the fields in displayed by the **show service-profile cac session** command.

Table 50. Output for show service-profile cac session

Field	Description
Service Profile	Name of the service profile
CAC Mode	CAC mode, either SESSION or NONE
Max Sessions	The number of CAC sessions available on UNIVERGE WL Access Points managed by this service profile.

See Also

- 1 **set service-profile cac-mode** on page 341
- 1 **set service-profile cac-session** on page 342

show voip max-sessions

Displays the number of sessions and per-session bandwidth that can be supported by a single radio, for a specific aggregate bandwidth.

Syntax `show voip max-sessions bw`

bw Aggregate bandwidth, in Kbps. The output shows the number of sessions and bandwidth per session that can be supported on a radio based on the *bw* you specify.

Defaults None.

Access Enabled.

Usage The *bw* value you enter is the aggregate bandwidth for all NEC VoIP sessions on a radio. The bandwidth values in the output are per individual session.

Examples The following command displays the maximum number of sessions and the effective bandwidth for each session possible for each configurable sample period, for a maximum of 500 Kbps of total reserved bandwidth per session.

PROMPT# show voip max-sessions 500

Codec	10ms		20ms		30ms		40ms	
G.711	4@	121.6	5@	92.8	6@	83.2	6@	78.4
G.729	7@	65.6	13@	36.8	18@	27.2	22@	22.4

Table 51 describes the fields in this display.

show voip summary

Chapter 12

Table 51. Output for show voip max-sessions

Field	Description
Codec	Compression and decompression scheme used for voice sessions.
10ms	Sample rate.
20ms	
30ms	
40ms	
sessions@ Kbps	For each codec and sample rate, the maximum number of sessions that can be supported on the radio and the bandwidth at which they can be supported.

See Also

- 1 **set radio-profile max-voip-bw** on page 313
- 1 **set radio-profile max-voip-sessions** on page 315

show voip summary

Displays the QoS mode and VoIP bandwidth information for UNIVERGE WL Access Points radios.

Syntax **show voip summary ap** *ap-number*

Defaults None.

Access Enabled.

Examples The following command displays summary VoIP information for UNIVERGE WL Access Points 2:

```
PROMPT# show voip summary ap 2
Port   Radio Radio   QoS   Min Rate   Effective   Max VOIP   Current VOIP
      Profile Mode  (Mb/s)    BW (Kb/s)  BW (Kb/s)  BW (Kb/s)
=====
AP     2     1 dang   EXT    1.0        500        371        0
AP     2     2 dang   EXT    1.0        500        371        0
```

Table 52 describes the fields in this display.

Table 52. Output for show voip summary

Field	Description
Port	UNIVERGE WL Access Points number.
Radio	Radio number.
Radio Profile	Radio that is managing the radio.
QoS Mode	<p>QoS mode configured on the radio profile:</p> <ul style="list-style-type: none"> • EXT—Voice Extension • SVP—SpectraLink Voice Priority • WMM—Wi-Fi Multimedia <p>Note: If the mode is SVP or WMM, the remaining fields are blank. They show information for bandwidth-based CAC, which is available only with the Voice Extension (EXT) QoS mode.</p>
Min Rate (Mb/s)	<p>Minimum client rate. The minimum client rate is the lowest mandatory data transmission rate among all service profiles mapped to this radio profile, for the radio type.</p> <p>Note: This parameter is not related to the min-client-rate that is configurable for RF Auto-Tuning.</p>
Effective Bw (Kb/s)	Total bandwidth reserved for each client. Bandwidth is reserved both for VoIP traffic and for management traffic.
Max VOIP BW (Kb/s)	Total bandwidth that is available per client specifically for VoIP traffic.
Current VOIP Bw (Kb/s)	Total aggregate bandwidth that is in use for all active VoIP sessions on the radio.

show voip summary

Chapter 12

See Also

- 1 **set radio-profile max-voip-bw** on page 313
- 1 **set radio-profile max-voip-sessions** on page 315

IGMP Snooping Commands

Use Internet Group Management Protocol (IGMP) snooping commands to configure and manage multicast traffic reduction on a UNIVERGE WL Controller. This chapter presents IGMP snooping commands alphabetically. Use the following table to locate commands in this chapter based on their use.

IGMP Snooping State	set igmp on page 428 show igmp on page 438
Proxy Reporting	set igmp proxy-report on page 433
Pseudo-querier	set igmp querier on page 436 show igmp querier on page 444
Timers	set igmp qi on page 433 set igmp oqi on page 432 set igmp qri on page 435 set igmp lmqi on page 429 set igmp rv on page 437
Router Solicitation	set igmp mrsol on page 430 set igmp mrsol mrsi on page 431
Multicast Routers	set igmp mrouter on page 430 show igmp mrouter on page 443
Multicast Receivers	set igmp receiver on page 436 show igmp receiver-table on page 446
Statistics	show igmp statistics on page 448 clear igmp statistics on page 428

clear igmp statistics

Clears IGMP statistics counters on one VLAN or all VLANs on a UNIVERGE WL Controller and resets them to 0.

Syntax **clear igmp statistics** [**vlan** *vlan-id*]

vlan *vlan-id* VLAN name or number. If you do not specify a VLAN, IGMP statistics are cleared for all VLANs.

Defaults None.

Access Enabled.

Examples The following command clears IGMP statistics for all VLANs:

```
PROMT# clear igmp statistics
IGMP statistics cleared for all vlans
```

See Also **show igmp statistics** on page 448

set igmp

Disables or reenables IGMP snooping on one VLAN or all VLANs on a UNIVERGE WL Controller.

Syntax **set igmp** {**enable** | **disable**} [**vlan** *vlan-id*]

enable Enables IGMP snooping.

disable Disables IGMP snooping.

vlan *vlan-id* VLAN name or number. If you do not specify a VLAN, IGMP snooping is disabled or reenabled on all VLANs.

Defaults IGMP snooping is enabled on all VLANs by default.

Access Enabled.

Examples The following command disables IGMP snooping on VLAN *orange*:

```
PROMT# set igmp disable vlan orange
```

success: change accepted.

See Also **show igmp** on page 438

set igmp lmqi

Changes the IGMP last member query interval timer on one VLAN or all VLANs on a UNIVERGE WL Controller.

Syntax **set igmp lmqi** *tenth-seconds* [**vlan** *vlan-id*]

lmqi *tenth-seconds* Amount of time (in tenths of a second) that the UNIVERGE WL Controller waits for a response to a group-specific query after receiving a leave message for that group, before removing the receiver that sent the leave message from the list of receivers for the group. If there are no more receivers for the group, the UNIVERGE WL Controller also sends a leave message for the group to multicast routers. You can specify a value from 1 through 65,535.

vlan *vlan-id* VLAN name or number. If you do not specify a VLAN, the timer change applies to all VLANs.

Defaults The default last member query interval is 10 tenths of a second (1 second).

Access Enabled.

Examples The following command changes the last member query interval on VLAN *orange* to 5 tenths of a second:

```
PROMT# set igmp lmqi 5 vlan orange
success: change accepted.
```

See Also

1 **set igmp oqi** on page 432

1 **set igmp qi** on page 433

1 **set igmp mrouter** on page 430

set igmp mrouter

Adds or removes a port in a UNIVERGE WL Controller list of ports on which it forwards traffic to multicast routers. Static multicast ports are immediately added to or removed from the list of router ports and do not age out.

Syntax `set igmp mrouter port port-list {enable | disable}`

port <i>port-list</i>	Port list. UNIVERGE WL Control System adds or removes the specified ports in the list of static multicast router ports.
enable	Adds the port to the list of static multicast router ports.
disable	Removes the port from the list of static multicast router ports.

Defaults By default, no ports are static multicast router ports.

Access Enabled.

Examples The following command adds port 1 as a static multicast router port:

```
PROMT# set igmp mrouter port 1enable
success: change accepted.
```

The following command removes port 1 from the static multicast router port list:

```
PROMT# set igmp mrouter port 1disable
success: change accepted.
```

See Also `show igmp mrouter` on page 443

set igmp mrsol

Enables or disables multicast router solicitation by a UNIVERGE WL Controller on one VLAN or all VLANs.

Syntax `set igmp mrsol {enable | disable} [vlan vlan-id]`

enable	Enables multicast router solicitation.
---------------	--

disable Disables multicast router solicitation.

vlan *vlan-id* VLAN name or number. If you do not specify a VLAN, multicast router solicitation is disabled or enabled on all VLANs.

Defaults Multicast router solicitation is disabled on all VLANs by default.

Access Enabled.

Examples The following command enables multicast router solicitation on VLAN *orange*:

```
PROMT# set igmp mrsol enable vlan orange
success: change accepted.
```

See Also **set igmp mrsol mrsi** on page 431

set igmp mrsol mrsi

Changes the interval between multicast router solicitations by a UNIVERGE WL Controller on one VLAN or all VLANs.

Syntax **set igmp mrsol mrsi** *seconds* [**vlan** *vlan-id*]

seconds Number of seconds between multicast router solicitations. You can specify a value from 1 through 65,535.

vlan *vlan-id* VLAN name or number. If you do not specify a VLAN, UNIVERGE WL Control System changes the multicast router solicitation interval for all VLANs.

Defaults The interval between multicast router solicitations is 30 seconds by default.

Access Enabled.

Examples The following example changes the multicast router solicitation interval to 60 seconds:

```
PROMT# set igmp mrsol mrsi 60
success: change accepted.
```

See Also **set igmp mrsol** on page 430

set igmp oqi

Changes the IGMP other-querier-present interval timer on one VLAN or all VLANs on a UNIVERGE WL Controller.

Syntax **set igmp oqi** *seconds* [**vlan** *vlan-id*]

oqi <i>seconds</i>	Number of seconds that the UNIVERGE WL Controller waits for a general query to arrive before electing itself the querier. You can specify a value from 1 through 65,535.
vlan <i>vlan-id</i>	VLAN name or number. If you do not specify a VLAN, the timer change applies to all VLANs.

Defaults The default other-querier-present interval is 255 seconds (4.25 minutes).

Access Enabled.

Usage A UNIVERGE WL Controller cannot become the querier unless the pseudo-querier feature is enabled on the UNIVERGE WL Controller. When the feature is enabled, the UNIVERGE WL Controller becomes the querier for a subnet so long as the UNIVERGE WL Controller does not receive a query message from a router with a lower IP address than the IP address of the UNIVERGE WL Controller in that subnet. To enable the pseudo-querier feature, use **set igmp querier**.

Examples The following command changes the other-querier-present interval on VLAN *orange* to 200 seconds:

```
PROMT# set igmp oqi 200 vlan orange
success: change accepted.
```

See Also

- 1 **set igmp lmqi** on page 429
- 1 **set igmp qi** on page 433
- 1 **set igmp qri** on page 435

- 1 **set igmp querier** on page 436
- 1 **set igmp mrouter** on page 430
- 1 **set igmp rv** on page 437

set igmp proxy-report

Disables or reenables proxy reporting by a UNIVERGE WL Controller on one VLAN or all VLANs.

Syntax **set igmp proxy-report** {**enable** | **disable**} [**vlan** *vlan-id*]

enable Enables proxy reporting.

disable Disables proxy reporting.

vlan *vlan-id* VLAN name or number. If you do not specify a VLAN, proxy reporting is disabled or reenabled on all VLANs.

Defaults Proxy reporting is enabled on all VLANs by default.

Access Enabled.

Usage Proxy reporting reduces multicast overhead by sending only one membership report for a group to the multicast routers and discarding other membership reports for the same group. If you disable proxy reporting, the UNIVERGE WL Controller sends all membership reports to the routers, including multiple reports for the same group.

Examples The following example disables proxy reporting on VLAN *orange*:

```
PROMT# set igmp proxy-report disable vlan orange
success: change accepted.
```

See Also **show igmp** on page 438

set igmp qi

Changes the IGMP query interval timer on one VLAN or all VLANs on a UNIVERGE WL Controller.

Syntax **set igmp qi** *seconds* [**vlan** *vlan-id*]

qi <i>seconds</i>	Number of seconds that elapse between general queries sent by the UNIVERGE WL Controller when the UNIVERGE WL Controller is the querier for the subnet. You can specify a value from 1 through 65,535.
vlan <i>vlan-id</i>	VLAN name or number. If you do not specify a VLAN, the timer change applies to all VLANs.

Defaults The default query interval is 125 seconds.

Access Enabled.

Usage The query interval is applicable only when the UNIVERGE WL Controller is querier for the subnet. For the UNIVERGE WL Controller to become the querier, the pseudo-querier feature must be enabled on the UNIVERGE WL Controller and the UNIVERGE WL Controller must have the lowest IP address among all the devices eligible to become a querier. To enable the pseudo-querier feature, use the **set igmp querier** command.

Examples The following command changes the query interval on VLAN *orange* to 100 seconds:

```
PROMT# set igmp qi 100 vlan orange
success: change accepted.
```

See Also

- 1 **set igmp lmqi** on page 429
- 1 **set igmp oqi** on page 432
- 1 **set igmp qri** on page 435
- 1 **set igmp querier** on page 436
- 1 **set igmp mrouter** on page 430
- 1 **set igmp rv** on page 437

set igmp qri

Changes the IGMP query response interval timer on one VLAN or all VLANs on a UNIVERGE WL Controller.

Syntax `set igmp qri tenth-seconds [vlan vlan-id]`

qri <i>tenth-seconds</i>	Amount of time (in tenths of a second) that the UNIVERGE WL Controller waits for a receiver to respond to a group-specific query message before removing the receiver from the receiver list for the group. You can specify a value from 1 through 65,535.
vlan <i>vlan-id</i>	VLAN name or number. If you do not specify a VLAN, the timer change applies to all VLANs.

Defaults The default query response interval is 100 tenths of a second (10 seconds).

Access Enabled.

Usage The query response interval is applicable only when the UNIVERGE WL Controller is querier for the subnet. For the UNIVERGE WL Controller to become the querier, the pseudo-querier feature must be enabled on the UNIVERGE WL Controller and the UNIVERGE WL Controller must have the lowest IP address among all the devices eligible to become a querier. To enable the pseudo-querier feature, use **set igmp querier**.

Examples The following command changes the query response interval on VLAN *orange* to 50 tenths of a second (5 seconds):

```
PROMT# set igmp qri 50 vlan orange
success: change accepted.
```

See Also

- 1 **set igmp lmqi** on page 429
- 1 **set igmp oqi** on page 432
- 1 **set igmp qi** on page 433
- 1 **set igmp querier** on page 436
- 1 **set igmp rv** on page 437

set igmp querier

Enables or disables the IGMP pseudo-querier on a UNIVERGE WL Controller , on one VLAN or all VLANs.

Syntax `set igmp querier {enable | disable} [vlan vlan-id]`

enable Enables the pseudo-querier.

disable Disables the pseudo-querier.

vlan *vlan-id* VLAN name or number. If you do not specify a VLAN, the pseudo-querier is enabled or disabled on all VLANs.

Defaults The pseudo-querier is disabled on all VLANs by default.

Access Enabled.

Usage UNIVERGE WL Control System recommends that you use the pseudo-querier only when the VLAN contains local multicast traffic sources and no multicast router is servicing the subnet.

Examples The following example enables the pseudo-querier on the *orange* VLAN:

```
PROMT# set igmp querier enable vlan orange
success: change accepted.
```

See Also `show igmp querier` on page 444

set igmp receiver

Adds or removes a network port in the list of ports on which a UNIVERGE WL Controller forwards traffic to multicast receivers. Static multicast receiver ports are immediately added to or removed from the list of receiver ports and do not age out.

Syntax **set igmp receiver port** *port-list* { **enable** | **disable** }

port <i>port-list</i>	Network port list. UNIVERGE WL Control System adds the specified ports to the list of static multicast receiver ports.
enable	Adds the port to the list of static multicast receiver ports.
disable	Removes the port from the list of static multicast receiver ports.

Defaults By default, no ports are static multicast receiver ports.

Access Enabled.

Examples The following command adds port 1 as a static multicast receiver port:

```
PROMT# set igmp receiver port 1 enable
success: change accepted.
```

The following command removes port 1 from the list of static multicast receiver ports:

```
PROMT# set igmp receiver port 1 disable
success: change accepted.
```

See Also **show igmp receiver-table** on page 446

set igmp rv

Changes the robustness value for one VLAN or all VLANs on a UNIVERGE WL Controller . Robustness adjusts the IGMP timers to the amount of traffic loss that occurs on the network.

Syntax **set igmp rv** *num* [**vlan** *vlan-id*]

<i>num</i>	Robustness value. You can specify a value from 2 through 255. Set the robustness value higher to adjust for more traffic loss.
vlan <i>vlan-id</i>	VLAN name or number. If you do not specify a VLAN, UNIVERGE WL Control System changes the robustness value for all VLANs.

show igmp

Chapter 13

Defaults The default robustness value for all VLANs is 2.

Access Enabled.

Examples The following example changes the robustness value on VLAN *orange* to 4:

```
PROMT# set igmp rv 4 vlan orange
success: change accepted.
```

See Also

- 1 **set igmp oqi** on page 432
- 1 **set igmp qi** on page 433
- 1 **set igmp qri** on page 435

show igmp

Displays IGMP configuration information and statistics for one VLAN or all VLANs.

Syntax **show igmp** [**vlan** *vlan-id*]

vlan *vlan-id* VLAN name or number. If you do not specify a VLAN, UNIVERGE WL Control System displays IGMP information for all VLANs.

Defaults None.

Access All.

Examples The following command displays IGMP information for VLAN *orange*:

```
PROMT# show igmp vlan orange
VLAN: orange
IGMP is enabled
Proxy reporting is on
Mrouter solicitation is on
Querier functionality is off
Configuration values: qi: 125 oqi: 300 qri: 100 lmqi: 10 rvalue: 2 Multicast

router information:
```

```

Port Mrouter-IPaddr Mrouter-MAC      Type  TTL
-----
  10      192.28.7.5 00:01:02:03:04:05 dvmrp  17
Group      Port Receiver-IP      Receiver-MAC      TTL
-----
    224.0.0.2 none          none          none undef
237.255.255.255 5      10.10.10.11 00:02:04:06:08:0b 258
237.255.255.255 5      10.10.10.13 00:02:04:06:08:0d 258
237.255.255.255 5      10.10.10.14 00:02:04:06:08:0e 258
237.255.255.255 5      10.10.10.12 00:02:04:06:08:0c 258
237.255.255.255 5      10.10.10.10 00:02:04:06:08:0a 258
Querier information:
Querier for vlan orange
Port Querier-IP      Querier-MAC      TTL
-----
  1 193.122.135.178 00:60:b9:11:e9:b4  23
IGMP vlan member ports: 10, 12, 11, 14, 16, 15, 13, 18, 17, 1, 20, 21, 2,
22, 19, 4, 6, 5, 3, 8, 7, 9
IGMP static ports: none
IGMP statistics for vlan orange:

```

```

IGMP message type Received Transmitted Dropped
-----
General-Queries      0          0          0
GS-Queries           0          0          0
Report V1            0          0          0
Report V2            5          1          4
Leave                 0          0          0
Mrouter-Adv          0          0          0
Mrouter-Term         0          0          0
Mrouter-Sol         50         101          0
DVMRP                4          4          0
PIM V1               0          0          0
PIM V2               0          0          0
Topology notifications: 0
Packets with unknown IGMP type: 0
Packets with bad length: 0
Packets with bad checksum: 0
Packets dropped: 4

```

Table 53 describes the fields in this display.

Table 53. Output for show igmp

Field	Description
VLAN	VLAN name. UNIVERGE WL Control System displays information separately for each VLAN.
IGMP is enabled (disabled)	IGMP state.
Proxy reporting	Proxy reporting state.
Mrouter solicitation	Multicast router solicitation state.
Querier functionality	Pseudo-querier state.
Configuration values (qi)	Query interval.
Configuration values (oqi)	Other-querier-present interval.
Configuration values (qri)	Query response interval.
Configuration values (lmqi)	Last member query interval.
Configuration values (rvalue)	Robustness value.
Multicast router information	List of multicast routers and active multicast groups. The fields containing this information are described separately. The show igmp mrouter command shows the same information.
Port	Number of the physical port through which the UNIVERGE WL Controller can reach the router.
Mrouter-IPaddr	IP address of the multicast router interface.
Mrouter-MAC	MAC address of the multicast router interface.

Table 53. Output for show igmp

Field	Description
Type	How the UNIVERGE WL Controller learned that the port is a multicast router port: <ul style="list-style-type: none"> • conf — Static multicast port configured by an administrator • madv—Multicast advertisement • quer—IGMP query • dvmrp—Distance Vector Multicast Routing Protocol (DVMRP) • pimv1—Protocol Independent Multicast (PIM) version 1 • pimv2—PIM version 2
TTL	Number of seconds before this entry ages out if not refreshed. For static multicast router entries, the time-to-live (TTL) value is <i>undef</i> . Static multicast router entries do not age out.
Group	IP address of a multicast group. The show igmp receiver-table command shows the same information as these receiver fields.
Port	Physical port through which the UNIVERGE WL Controller can reach the group's receiver.
Receiver-IP	IP address of the client receiving the group.
Receiver-MAC	MAC address of the client receiving the group.
TTL	Number of seconds before this entry ages out if the UNIVERGE WL Controller does not receive a group membership message from the receiver. For static multicast receiver entries, the TTL value is <i>undef</i> . Static multicast receiver entries do not age out.

Table 53. Output for show igmp

Field	Description
Querier information	Information about the subnet's multicast querier. If the querier is another device, the fields described below are applicable. If the querier is the UNIVERGE WL Controller itself, the output indicates how many seconds remain until the next general query message. If IGMP snooping does not detect a querier, the output indicates this. The show igmp querier command shows the same information.
Querier for vlan	VLAN containing the querier. Information is listed separately for each VLAN.
Querier-IP	IP address of the querier.
Querier-MAC	MAC address of the querier.
TTL	Number of seconds before this entry ages out if the UNIVERGE WL Controller does not receive a query message from the querier.
IGMP vlan member ports	Physical ports in the VLAN. This list includes all network ports configured to be in the VLAN and all ports UNIVERGE WL Control System dynamically assigns to the VLAN when a user assigned to the VLAN becomes a receiver.
IGMP static ports	Static receiver ports.
IGMP statistics	Multicast message and packet statistics. These are the same statistics displayed by the show igmp statistics command.

See Also

- 1 **show igmp mrouter** on page 443
- 1 **show igmp querier** on page 444
- 1 **show igmp receiver-table** on page 446
- 1 **show igmp statistics** on page 448

show igmp mrouter

Displays the multicast routers in a UNIVERGE WL Controller subnet, on one VLAN or all VLANs. Routers are listed separately for each VLAN, according to the port number through which the UNIVERGE WL Controller can reach the router.

Syntax `show igmp mrouter [vlan vlan-id]`

vlan *vlan-id* VLAN name or number. If you do not specify a VLAN, UNIVERGE WL Control System displays the multicast routers in all VLANs.

Defaults None.

Access All.

Examples The following command displays the multicast routers in VLAN *orange*:

```
PROMT# show igmp mrouter vlan orange
Multicast routers for vlan orange
Port Mrouter-IPAddr  Mrouter-MAC      Type  TTL
-----
  10      192.28.7.5 00:60:b9:11:04:05 dvmrp   33
```

Table 54 describes the fields in this display.

Table 54. Output for show igmp mrouter

Field	Description
Multicast routers for vlan	VLAN containing the multicast routers. Ports are listed separately for each VLAN.
Port	Number of the physical port through which the UNIVERGE WL Controller can reach the router.
Mrouter-IPAddr	IP address of the multicast router.
Mrouter-MAC	MAC address of the multicast router.

Table 54. Output for show igmp mrouter

Field	Description
Type	How the UNIVERGE WL Controller learned that the port is a multicast router port: <ul style="list-style-type: none">• conf — Static multicast port configured by an administrator• madv—Multicast advertisement• quer—IGMP query• dvmrp—Distance Vector Multicast Routing Protocol (DVMRP)• pimv1—Protocol Independent Multicast (PIM) version 1• pimv2—PIM version 2
TTL	Number of seconds before this entry ages out if unused. For static multicast router entries, the TTL value is <i>undef</i> . Static multicast router entries do not age out.

See Also

- 1 **set igmp mrouter** on page 430
- 1 **show igmp mrouter** on page 443

show igmp querier

Displays information about the active multicast querier, on one VLAN or all VLANs. Queriers are listed separately for each VLAN. Each VLAN can have only one querier.

Syntax **show igmp querier** [**vlan** *vlan-id*]

vlan *vlan-id* VLAN name or number. If you do not specify a VLAN, UNIVERGE WL Control System displays querier information for all VLANs.

Defaults None.

Access Enabled.

Examples The following command displays querier information for VLAN *orange*:

```
PROMT# show igmp querier vlan orange
Querier for vlan orange
Port Querier-IP      Querier-MAC      TTL
-----
1 193.122.135.178 00:60:b9:11:e9:b4 23
```

The following command shows the information UNIVERGE WL Control System displays when the querier is the UNIVERGE WL Controller itself:

```
PROMT# show igmp querier vlan default
Querier for vlan default:
I am the querier for vlan default, time to next query is 20
```

The output indicates how many seconds remain before the pseudo-querier on the UNIVERGE WL Controller broadcasts the next general query report to IP address 224.0.0.1, the multicast all-systems group.

If IGMP snooping does not detect a querier, the output indicates this finding, as shown in the following example:

```
PROMT# show igmp querier vlan red
Querier for vlan red:
There is no querier present on vlan red
```

This condition does not necessarily indicate a problem. For example, election of the querier might be in progress.

Table 55 on page 446 describes the fields in the display when a querier other than the UNIVERGE WL Controller is present.

Table 55. Output for show igmp querier

Field	Description
Querier for vlan	VLAN containing the querier. Information is listed separately for each VLAN.
Querier-IP	IP address of the querier interface.
Querier-MAC	MAC address of the querier interface.
TTL	Number of seconds before this entry ages out if the UNIVERGE WL Controller does not receive a query message from the querier.

See Also `set igmp querier` on page 436

show igmp receiver-table

Displays the receivers to which a UNIVERGE WL Controller forwards multicast traffic. You can display receivers for all VLANs, a single VLAN, or a group or groups identified by group address and network mask.

Syntax `show igmp receiver-table [vlan vlan-id] [group group-ip-addr/mask-length]`

vlan *vlan-id* VLAN name or number. If you do not specify a VLAN, UNIVERGE WL Control System displays the multicast receivers on all VLANs.

group *group-ip-addr/mask-length* IP address and subnet mask of a multicast group, in CIDR format (for example, 239.20.20.10/24). If you do not specify a group address, UNIVERGE WL Control System displays the multicast receivers for all groups.

Defaults None.

Access All.

Examples The following command displays all multicast receivers in VLAN *orange*:

```
PROMT# show igmp receiver-table vlan orange
VLAN: orange
Session      Port Receiver-IP      Receiver-MAC      TTL
-----
224.0.0.2    none                none              none             undef
237.255.255.255  5      10.10.10.11 00:60:b9:11:08:0b 179
237.255.255.255  5      10.10.10.13 00:60:b9:11:08:0d 179
237.255.255.255  5      10.10.10.14 00:60:b9:11:08:0e 179
237.255.255.255  5      10.10.10.12 00:60:b9:11:08:0c 179
237.255.255.255  5      10.10.10.10 00:60:b9:11:08:0a 179
```

The following command lists all receivers for multicast groups 237.255.255.1 through 237.255.255.255, in all VLANs:

```
PROMT# show igmp receiver-table group 237.255.255.0/24
VLAN: red
Session      Port Receiver-IP      Receiver-MAC      TTL
-----
237.255.255.2    2      10.10.20.19 00:60:b9:11:09:0d 112
237.255.255.119  3      10.10.30.31 00:60:b9:11:01:0b 112

VLAN: green
Session      Port Receiver-IP      Receiver-MAC      TTL
-----
237.255.255.17    11     10.10.40.41 00:60:b9:11:02:0c 12
237.255.255.255    6     10.10.60.61 00:60:b9:11:0a:01 111
```

Table 56 describes the fields in this display.

Table 56. Output for show igmp receiver-table

Field	Description
VLAN	VLAN that contains the multicast receiver ports. Ports are listed separately for each VLAN.
Session	IP address of the multicast group being received.
Port	Physical port through which the UNIVERGE WL Controller can reach the receiver.
Receiver-IP	IP address of the receiver.

show igmp statistics

Chapter 13

Table 56. Output for show igmp receiver-table

Field	Description
Receiver-MAC	MAC address of the receiver.
TTL	Number of seconds before this entry ages out if the UNIVERGE WL Controller does not receive a group membership message from the receiver. For static multicast receiver entries, the TTL value is <i>undef</i> . Static multicast receiver entries do not age out.

See Also `set igmp receiver` on page 436

show igmp statistics

Displays IGMP statistics.

Syntax `show igmp statistics [vlan vlan-id]`

vlan *vlan-id* VLAN name or number. If you do not specify a VLAN, UNIVERGE WL Control System displays IGMP statistics for all VLANs.

Defaults None.

Access All.

Examples The following command displays IGMP statistics for VLAN *orange*:

```
PROMT# show igmp statistics vlan orange
IGMP statistics for vlan orange:
```

IGMP message type	Received	Transmitted	Dropped
General-Queries	0	0	0
GS-Queries	0	0	0
Report V1	0	0	0
Report V2	5	1	4
Leave	0	0	0
Mrouter-Adv	0	0	0
Mrouter-Term	0	0	0

```

Mrouter-Sol          50          101          0
DVMRP                 4           4           0
PIM V1                0           0           0
PIM V2                0           0           0
Topology notifications: 0
Packets with unknown IGMP type: 0
Packets with bad length: 0
Packets with bad checksum: 0
Packets dropped: 4

```

Table 57 describes the fields in this display.

Table 57. Output for show igmp statistics

Field	Description
IGMP statistics for vlan	VLAN name. Statistics are listed separately for each VLAN.
IGMP message type	Type of IGMP message: <ul style="list-style-type: none"> • General-Queries—General group membership queries sent by the multicast querier (multicast router or pseudo-querier). • GS-Queries—Group-specific queries sent by the the multicast querier to determine whether there are receivers for a specific group. • Report V1—IGMP version 1 group membership reports sent by clients who want to be receivers for the groups. • Report V2—IGMP version 2 group membership reports sent by clients who want to be receivers for the groups. • Leave—IGMP version 2 leave messages sent by clients who want to stop receiving traffic for a group. Leave messages apply only to IGMP version 2. • Mrouter-Adv—Multicast router advertisement packets. A multicast router sends this type of packet to advertise the IP address of the sending interface as a multicast router interface.

Table 57. Output for show igmp statistics

Field	Description
IGMP message type	Type of IGMP message, continued: <ul style="list-style-type: none"> • Mrouter-Term—Multicast router termination messages. A multicast router sends this type of message when multicast forwarding is disabled on the router interface, the router interface is administratively disabled, or the router itself is gracefully shutdown. • Mrouter-Sol—Multicast router solicitation messages. A multicast client or a UNIVERGE WL Controller sends this type of message to immediately solicit multicast router advertisement messages from the multicast routers in the subnet. • DVMRP—Distance Vector Multicast Routing Protocol (DVMRP) messages. Multicast routers running DVMRP exchange multicast information with these messages. • PIM V1—Protocol Independent Multicast (PIM) version 1 messages. Multicast routers running PIMv1 exchange multicast information with these messages. • PIM V2—PIM version 2 messages.
Received	Number of packets received.
Transmitted	Number of packets transmitted. This number includes both multicast packets originated by the UNIVERGE WL Controller and multicast packets received and then forwarded by the UNIVERGE WL Controller.
Dropped	Number of IGMP packets dropped by the UNIVERGE WL Controller.
Topology notifications	Number of Layer 2 topology change notifications received by the UNIVERGE WL Controller.
	Note: In the UNIVERGE WL Control System, the value in this field is always 0.

Table 57. Output for show igmp statistics

Field	Description
Packets with unknown IGMP type	Number of multicast packets received with an unrecognized multicast type.
Packets with bad length	Number of packets with an invalid length.
Packets with bad IGMP checksum	Number of packets with an invalid IGMP checksum value.
Packets dropped	Number of multicast packets dropped by the UNIVERGE WL Controller.

See Also `clear igmp statistics` on page 428

show igmp statistics
Chapter 13

Security ACL Commands

Use security ACL commands to configure and monitor security access control lists (ACLs). Security ACLs filter packets to restrict or permit network usage by certain users or traffic types, and can assign to packets a class of service (CoS) to define the priority of treatment for packet filtering.

(Security ACLs are different from the location policy on a UNIVERGE WL Controller, which helps you locally control user access. For location policy commands, see Chapter 9, “AAA Commands,” on page 183.)

This chapter presents security ACL commands alphabetically. Use the following table to locate commands in this chapter based on their use.

Create Security ACLs	set security acl on page 460
	show security acl editbuffer on page 471
	show security acl info on page 473
	show security acl on page 470
	clear security acl on page 454
Commit Security ACLs	commit security acl on page 458
	rollback security acl on page 459
Map Security ACLs	set security acl map on page 467
	show security acl map on page 474
	clear security acl map on page 456
Monitor Security ACLs	show security acl hits on page 472
	set security acl hit-sample-rate on page 469
	show security acl resource-usage on page 475

clear security acl

Clears a specified security ACL, an access control entry (ACE), or all security ACLs, from the edit buffer. When used with the command **commit security acl**, clears the ACE from the running configuration.

Syntax **clear security acl** { *acl-name* | **all** } [*editbuffer-index*]

<i>acl-name</i>	Name of an existing security ACL to clear. ACL names start with a letter and are case-insensitive.
all	Clears all security ACLs.
<i>editbuffer-index</i>	Number that indicates which access control entry (ACE) in the security ACL to clear. If you do not specify an ACE, all ACEs are cleared from the ACL.

Defaults None.

Access Enabled.

Usage This command deletes security ACLs only in the edit buffer. You must use the **commit security acl** command with this command to delete the ACL or ACE from the running configuration and nonvolatile storage.

The **clear security acl** command deletes a security ACL, but does not stop its current filtering function if the ACL is mapped to any virtual LANs (VLANs), ports, or virtual ports, or if the ACL is applied in a Filter-Id attribute to an authenticated user or group of users with current sessions.

Examples The following commands display the current security ACL configuration, clear *acl_133* in the edit buffer, commit the deletion to the running configuration, and redisplay the ACL configuration to show that it no longer contains *acl_133*:

```
PROMPT# show security acl info all
ACL information for all
set security acl ip acl_133 (hits #1 0)
-----
1. deny IP source IP 192.168.1.6 0.0.0.0 destination IP any
set security acl ip acl_134 (hits #3 0)
-----
1. permit IP source IP 192.168.0.1 0.0.0.0 destination IP any enable-hits
```

```
set security acl ip acl_135 (hits #2 0)
-----
1. deny IP source IP 192.168.1.1 0.0.0.0 destination IP any enable-hits
PROMPT# clear security acl acl_133
PROMPT# commit security acl acl_133
configuration accepted
PROMPT# show security acl info all
ACL information for all
set security acl ip acl_134 (hits #3 0)
-----
1. permit IP source IP 192.168.0.1 0.0.0.0 destination IP any enable-hits
set security acl ip acl_135 (hits #2 0)
-----
1. deny IP source IP 192.168.1.1 0.0.0.0 destination IP any enable-hits
```

See Also

- 1 **clear security acl map** on page 456
- 1 **commit security acl** on page 458
- 1 **set security acl** on page 460
- 1 **show security acl info** on page 473

clear security acl map

Deletes the mapping between a security ACL and a virtual LAN (VLAN), one or more physical ports, or a virtual port. Or deletes all ACL maps to VLANs, ports, and virtual ports on a UNIVERGE WL Controller.



Note. Security ACLs are applied to users or groups dynamically via the Filter-Id attribute. To delete a security ACL from a user or group in the local UNIVERGE WL Controller database, use the command **clear user attr**, **clear mac-user attr**, **clear usergroup attr**, or **clear mac-usergroup attr**. To delete a security ACL from a user or group on an external RADIUS server, see the documentation for your RADIUS server.

Syntax **clear security acl map** {*acl-name* | **all**} {**vlan** *vlan-id* | **port** *port-list* [*tag tag-value*] | **ap** *ap-num*} {**in** | **out**}

<i>acl-name</i>	Name of an existing security ACL to clear. ACL names start with a letter and are case-insensitive.
all	Removes security ACL mapping from all physical ports, virtual ports, and VLANs on a UNIVERGE WL Controller.
vlan <i>vlan-id</i>	VLAN name or number. UNIVERGE WL Control System removes the security ACL from the specified VLAN.
port <i>port-list</i>	Port list. UNIVERGE WL Control System removes the security ACL from the specified UNIVERGE WL Controller physical port or ports.
tag <i>tag-value</i>	Tag value that identifies a virtual port in a VLAN. Specify a value from 1 through 4093. UNIVERGE WL Control System removes the security ACL from the specified virtual port.

ap <i>ap-num</i>	One or more UNIVERGE WL Access Points, based on their connection IDs. Specify a single connection ID, or specify a comma-separated list of connection IDs, a hyphen-separated range, or any combination, with no spaces. UNIVERGE WL Control System removes the security ACL from the specified UNIVERGE WL Access Points.
in	Removes the security ACL from traffic coming <i>into</i> the UNIVERGE WL Controller.
out	Removes the security ACL from traffic going <i>out of</i> the UNIVERGE WL Controller.

Defaults None.

Access Enabled.

Usage To clear a security ACL map, type the name of the ACL with the VLAN, physical port or ports, virtual port tag, or UNIVERGE WL Access Points and the direction of the packets to stop filtering. This command deletes the ACL mapping, but not the ACL.

Examples To clear the mapping of security ACL *acljoe* from port 1 for incoming packets, type the following command:

```
PROMPT# clear security acl map acljoe port 1 in
clear mapping accepted
```

To clear all physical ports, virtual ports, and VLANs on a UNIVERGE WL Controller of the ACLs mapped for incoming and outgoing traffic, type the following command:

```
PROMPT# clear security acl map all
success: change accepted.
```

See Also

- 1 **clear security acl** on page 454
- 1 **set security acl map** on page 467
- 1 **show security acl map** on page 474

commit security acl

Saves a security ACL, or all security ACLs, in the edit buffer to the running configuration and nonvolatile storage on the UNIVERGE WL Controller. Or, when used with the **clear security acl** command, **commit security acl** deletes a security ACL, or all security ACLs, from the running configuration and nonvolatile storage.

Syntax **commit security acl** {*acl-name* | **all**}

acl-name Name of an existing security ACL to commit. ACL names must start with a letter and are case-insensitive.

all Commits all security ACLs in the edit buffer.

Defaults None.

Access Enabled.

Usage Use the **commit security acl** command to save security ACLs into, or delete them from, the permanent configuration. Until you commit the creation or deletion of a security ACL, it is stored in an edit buffer and is not enforced. After you commit a security ACL, it is removed from the edit buffer.

A single **commit security acl all** command commits the creation and/or deletion of whatever **show security acl info all editbuffer** shows to be currently stored in the edit buffer.

Examples The following commands commit all the security ACLs in the edit buffer to the configuration, display a summary of the committed ACLs, and show that the edit buffer has been cleared:

```
PROMPT# commit security acl all
configuration accepted
PROMPT# show security acl
ACL table
ACL                               Type  Class  Mapping
-----
acl_123                           IP     Static
acl_124                           IP     Static
PROMPT# show security acl info all editbuffer
acl editbuffer information for all
```

See Also

- 1 **clear security acl** on page 454
- 1 **rollback security acl** on page 459
- 1 **set security acl** on page 460
- 1 **show security acl** on page 470
- 1 **show security acl info** on page 473

rollback security acl

Clears changes made to the security ACL edit buffer since it was last saved. The ACL is rolled back to its state after the last **commit security acl** command was entered. All uncommitted ACLs in the edit buffer are cleared.

Syntax **rollback security acl** {*acl-name* | **all**}

acl-name Name of an existing security ACL to roll back. ACL names must start with a letter and are case-insensitive.

all Rolls back all security ACLs in the edit buffer, clearing all uncommitted ACEs.

Defaults None.

Access Enabled.

Examples The following commands show the edit buffer before a rollback, clear any changes in the edit buffer to security *acl_122*, and show the edit buffer after the rollback:

```
PROMPT# show security acl info all editbuffer
ACL edit-buffer information for all
set security acl ip acl_122 (ACEs 3, add 3, del 0, modified 0)
-----
1. permit IP source IP 20.0.1.11 0.0.0.255 destination IP any enable-hits
2. deny IP source IP 20.0.2.11 0.0.0.0 destination IP any
```

```
3. deny SRC source IP 192.168.1.234 255.255.255.255 enable-hits
PROMPT# rollback security acl acl_122
PROMPT# show security acl info all editbuffer
ACL edit-buffer information for all
```

See Also `show security acl` on page 470

set security acl

In the edit buffer, creates a security access control list (ACL), adds one access control entry (ACE) to a security ACL, and/or reorders ACEs in the ACL. The ACEs in an ACL filter IP packets by source IP address, a Layer 4 protocol, or IP, ICMP, TCP, or UDP packet information.

Syntax

By source address

```
set security acl ip acl-name {permit [cos cos] | deny} {source-ip-addr mask | any} [before editbuffer-index | modify editbuffer-index] [hits]
```

By Layer 4 protocol

```
set security acl ip acl-name {permit [cos cos] | deny} protocol-number {source-ip-addr mask | any} {destination-ip-addr mask | any} [[precedence precedence] [tos tos] | [dscp codepoint]] [before editbuffer-index | modify editbuffer-index] [hits]
```

By IP packets

```
set security acl ip acl-name {permit [cos cos] | deny} ip {source-ip-addr mask | any} {destination-ip-addr mask | any} [[precedence precedence] [tos tos] | [dscp codepoint]] [before editbuffer-index | modify editbuffer-index] [hits]
```

By ICMP packets

```
set security acl ip acl-name {permit [cos cos] | deny} icmp {source-ip-addr
mask | any} {destination-ip-addr mask | any} [type icmp-type] [code icmp-code]
[[precedence precedence] [tos tos] | [dscp codepoint]]
[before editbuffer-index | modify editbuffer-index] [hits]
```

By TCP packets

```
set security acl ip acl-name {permit [cos cos] | deny}
tcp {source-ip-addr mask | any [operator port [port2]]}
{destination-ip-addr mask | any [operator port [port2]]}
[[precedence precedence] [tos tos] | [dscp codepoint]]
[established] [before editbuffer-index | modify editbuffer-index] [hits]
```

By UDP packets

```
set security acl ip acl-name {permit [cos cos] | deny} udp {source-ip-addr mask
| any [operator port [port2]]} {destination-ip-addr mask | any [operator port
[port2]]} [[precedence precedence] [tos tos] | [dscp codepoint]]
[before editbuffer-index | modify editbuffer-index] [hits]
```

acl-name

Security ACL name. ACL names must be unique within the UNIVERGE WL Controller, must start with a letter, and are case-insensitive. Specify an ACL name of up to 32 of the following characters:

- Letters *a* through *z* and *A* through *Z*
- Numbers 0 through 9
- Hyphen (-), underscore (_), and period (.)

UNIVERGE WL Control System recommends that you do not use the same name with different capitalizations for ACLs. For example, do not configure two separate ACLs with the names *acl_123* and *ACL_123*.

Note: In an ACL name, do *not* include the term **all**, **default-action**, **map**, **help**, or **editbuffer**.

permit

Allows traffic that matches the conditions in the ACE.

cos *cos*

For permitted packets, a class-of-service (CoS) level for packet handling. Specify a value from 0 through 7:

- **1** or **2**—Background. Packets are queued in UNIVERGE WL Access Points forwarding queue 4.
- **0** or **3**—Best effort. Packets are queued in UNIVERGE WL Access Points forwarding queue 3.
- **4** or **5**—Video. Packets are queued in UNIVERGE WL Access Points forwarding queue 2.

Use CoS level 4 or 5 for voice over IP (VoIP) packets other than SpectraLink Voice Priority (SVP).

- **6** or **7**—Voice. Packets are queued in UNIVERGE WL Access Points forwarding queue 1.

Use 6 or 7 only for VoIP phones that use SVP, not for other types of traffic

deny

protocol

Blocks traffic that matches the conditions in the ACE.

IP protocol by which to filter packets:

- **ip**
- **tcp**
- **udp**
- **icmp**
- A protocol number between 0 and 255.

(For a complete list of IP protocol names and numbers, see www.iana.org/assignments/protocol-numbers.)

source-ip-addr mask
| **any**

IP address and wildcard mask of the network or host *from* which the packet is being sent. Specify both address and mask in dotted decimal notation. For more information, see “Wildcard Masks” on page 8.

To match on any address, specify **any** or **0.0.0.0 255.255.255.255**.

<i>operator port [port2]</i>	<p>Operand and port number(s) for matching TCP or UDP packets to the number of the source or destination port on <i>source-ip-addr</i> or <i>destination-ip-addr</i>. Specify one of the following operands and the associated port:</p> <ul style="list-style-type: none">• eq—Packets are filtered for only <i>port</i> number.• gt—Packets are filtered for all ports that are greater than <i>port</i> number.• lt—Packets are filtered for all ports that are less than <i>port</i> number.• neq—Packets are filtered for all ports except <i>port</i> number.• range—Packets are filtered for ports in the range between <i>port</i> and <i>port2</i>. To specify a port range, enter two port numbers. Enter the lower port number first, followed by the higher port number. <p>(For a complete list of TCP and UDP port numbers, see www.iana.org/assignments/port-numbers.)</p>
<i>destination-ip-addr mask any</i>	<p>IP address and wildcard mask of the network or host to which the packet is being sent. Specify both address and mask in dotted decimal notation. For more information, see “Wildcard Masks” on page 8.</p> <p>To match on any address, specify any or 0.0.0.0 255.255.255.255.</p>
type <i>icmp-type</i>	<p>Filters ICMP messages by type. Specify a value from 0 through 255. (For a list of ICMP message type and code numbers, see www.iana.org/assignments/icmp-parameters.)</p>
code <i>icmp-code</i>	<p>For ICMP messages filtered by type, additionally filters ICMP messages by code. Specify a value from 0 through 255. (For a list of ICMP message type and code numbers, see www.iana.org/assignments/icmp-parameters.)</p>

precedence
precedence

Filters packets by precedence level. Specify a value from 0 through 7:

- **0**—routine precedence
- **1**—priority precedence
- **2**—immediate precedence
- **3**—flash precedence
- **4**—flash override precedence
- **5**—critical precedence
- **6**—internetwork control precedence
- **7**—network control precedence

tos tos

Filters packets by type of service (TOS) level. Specify one of the following values, or any sum of these values up to 15. For example, a **tos** value of **9** filters packets with the TOS levels minimum delay (**8**) and minimum monetary cost (**1**).

- **8**—minimum delay
- **4**—maximum throughput
- **2**—maximum reliability
- **1**—minimum monetary cost
- **0**—normal

dscp codepoint

Filters packets by Differentiated Services Code Point (DSCP) value. You can specify a number from 0 to 63, in decimal or binary format.

Note: You cannot use the **dscp** option along with the **precedence** and **tos** options in the same ACE. The CLI rejects an ACE that has this combination of options.

established

For TCP packets only, applies the ACE only to established TCP sessions and not to new TCP sessions.

before editbuffer-index

Inserts the new ACE in front of another ACE in the security ACL. Specify the number of the existing ACE in the edit buffer. Index numbers start at 1. (To display the edit buffer, use **show security acl editbuffer**.)

modify <i>editbuffer-index</i>	Replaces an ACE in the security ACL with the new ACE. Specify the number of the existing ACE in the edit buffer. Index numbers start at 1. (To display the edit buffer, use show security acl editbuffer .)
hits	Tracks the number of packets that are filtered based on a security ACL, for all mappings.

Defaults By default, permitted packets are classified based on DSCP value, which is converted into an internal CoS value in the UNIVERGE WL Controllers CoS map. The packet is then marked with a DSCP value based on the internal CoS value. If the ACE contains the **cos** option, this option overrides the UNIVERGE WL Controllers CoS map and marks the packet based on the ACE.

Access Enabled.

Usage The UNIVERGE WL Controller does not apply security ACLs until you activate them with the **commit security acl** command and map them to a VLAN, port, or virtual port, or to a user. If the UNIVERGE WL Controller is reset or restarted, any ACLs in the edit buffer are lost.

You cannot perform ACL functions that include permitting, denying, or marking with a Class of Service (CoS) level on packets with a multicast or broadcast destination address.

The order of security ACEs in a security ACL is important. Once an ACL is active, its ACEs are checked according to their order in the ACL. If an ACE criterion is met, its action takes place and any ACEs that follow are ignored.

ACEs are listed in the order in which you create them, unless you move them. To position security ACEs within a security ACL, use **before editbuffer-index** and **modify editbuffer-index**.

Examples The following command adds an ACE to security *acl_123* that permits packets from IP address 192.168.1.11/24 and counts the hits:

```
PROMPT# set security acl ip acl_123 permit 192.168.1.11 0.0.0.255 hits
```

The following command adds an ACE to *acl_123* that denies packets from IP address 192.168.2.11:

```
PROMPT# set security acl ip acl_123 deny 192.168.2.11 0.0.0.0
```

set security acl

Chapter 14

The following command creates *acl_125* by defining an ACE that denies TCP packets from source IP address 192.168.0.1 to destination IP address 192.168.0.2 for established sessions only, and counts the hits:

```
PROMPT# set security acl ip acl_125 deny tcp 192.168.0.1 0.0.0.0 192.168.0.2
0.0.0.0 established hits
```

The following command adds an ACE to *acl_125* that denies TCP packets from source IP address 192.168.1.1 to destination IP address 192.168.1.2, on destination port 80 only, and counts the hits:

```
PROMPT# set security acl ip acl_125 deny tcp 192.168.1.1 0.0.0.0 192.168.1.2
0.0.0.0 eq 80 hits
```

Finally, the following command commits the security ACLs in the edit buffer to the configuration:

```
PROMPT# commit security acl all
configuration accepted
```

See Also

- 1 **clear security acl** on page 454
- 1 **commit security acl** on page 458
- 1 **show security acl** on page 470

set security acl map

Assigns a committed security ACL to a VLAN, physical port or ports, virtual port, or UNIVERGE WL Access Points on the UNIVERGE WL Controller.



Note. To assign a security ACL to a user or group in the local UNIVERGE WL Controller database, use the command **set user attr**, **set mac-user attr**, **set usergroup attr**, or **set mac-usergroup attr** with the Filter-Id attribute. To assign a security ACL to a user or group with Filter-Id on a RADIUS server, see the documentation for your RADIUS server.

Syntax **set security acl map** *acl-name* { **vlan** *vlan-id* | **port** *port-list* [**tag** *tag-list*] | **ap** *ap-num* } { **in** | **out** }

<i>acl-name</i>	Name of an existing security ACL to map. ACL names start with a letter and are case-insensitive.
vlan <i>vlan-id</i>	VLAN name or number. UNIVERGE WL Control System assigns the security ACL to the specified VLAN.
port <i>port-list</i>	Port list. UNIVERGE WL Control System assigns the security ACL to the specified physical UNIVERGE WL Controller port or ports.
tag <i>tag-list</i>	One or more values that identify a virtual port in a VLAN. Specify a single tag value from 1 through 4093. Or specify a comma-separated list of values, a hyphen-separated range, or any combination, with no spaces. UNIVERGE WL Control System assigns the security ACL to the specified virtual port or ports.
ap <i>ap-num</i>	One or more UNIVERGE WL Access Points, based on their connection IDs. Specify a single connection ID, or specify a comma-separated list of connection IDs, a hyphen-separated range, or any combination, with no spaces. UNIVERGE WL Control System assigns the security ACL to the specified UNIVERGE WL Access Points.

set security acl map

Chapter 14

in	Assigns the security ACL to traffic coming <i>into</i> the UNIVERGE WL Controller.
out	Assigns the security ACL to traffic coming <i>from</i> the UNIVERGE WL Controller.

Defaults None.

Access Enabled.

Usage Before you can map a security ACL, you must use the **commit security acl** command to save the ACL in the running configuration and nonvolatile storage.

For best results, map only one input security ACL and one output security ACL to each VLAN, physical port, virtual port, or UNIVERGE WL Access Points to filter a flow of packets. If more than one security ACL filters the same traffic, UNIVERGE WL Control System applies only the first ACL match and ignores any other matches.

Examples The following command maps security ACL *acl_133* to ap 2 for incoming packets:

```
PROMPT# set security acl map acl_133 ap 2 in
success: change accepted.
```

See Also

- 1 **clear security acl map** on page 456
- 1 **commit security acl** on page 458
- 1 **set mac-user attr** on page 222
- 1 **set mac-usergroup attr** on page 230
- 1 **set security acl** on page 460
- 1 **set user attr** on page 236
- 1 **set usergroup** on page 238
- 1 **show security acl map** on page 474

set security acl hit-sample-rate

Specifies the time interval, in seconds, at which the packet counter for each security ACL is sampled for display. The counter counts the number of packets filtered by the security ACL—or “hits.”

Syntax `set security acl hit-sample-rate seconds`

seconds Number of seconds between samples. A sample rate of 0 (zero) disables the sample process.

Defaults By default, the hits are not sampled.

Access Enabled.

Usage To view counter results for a particular ACL, use the **show security acl info *acl-name*** command. To view the hits for all security ACLs, use the **show security acl hits** command.

Examples The first command sets UNIVERGE WL Control System to sample ACL hits every 15 seconds. The second and third commands display the results. The results show that 916 packets matching security *acl_153* were sent since the ACL was mapped.

```
PROMPT# set security acl hit-sample-rate 15
PROMPT# show security acl info acl_153
ACL information for acl_153
set security acl ip acl_153 (hits #3 916)
-----
1. permit IP source IP 20.1.1.1 0.0.0.0 destination IP any enable-hits
PROMPT# show security acl hits
ACL hit counters
Index Counter          ACL-name
-----
1           0 acl_2
2           0 acl_175
3          916 acl_153
```

See Also

- 1 **show security acl hits** on page 472
- 1 **show security acl info** on page 473

show security acl

Displays a summary of the security ACLs that are mapped.

Syntax **show security acl**

Defaults None.

Access Enabled.

Usage This command lists only the ACLs that have been mapped to something (a user, or VLAN, or port, and so on). To list all committed ACLs, use the **show security acl info** command. To list ACLs that have not yet been committed, use the **show security acl editbuffer** command.

Examples To display a summary of the mapped security ACLs on a UNIVERGE WL Controller, type the following command:

```
PROMPT# show security acl
```

```
ACL table
```

ACL	Type	Class	Mapping
acl_123	IP	Static	ap 2 In
acl_133	IP	Static	ap 4 In
acl_124	IP	Static	

See Also

- 1 **clear security acl** on page 454
- 1 **commit security acl** on page 458
- 1 **set security acl** on page 460
- 1 **show security acl editbuffer** on page 471
- 1 **show security acl info** on page 473

show security acl editbuffer

Displays a summary of the security ACLs that have not yet been committed to the configuration.

Syntax `show security acl [info all] editbuffer`

info all Displays the ACEs in each uncommitted ACL. Without this option, only the ACE names are listed.

Defaults None.

Access Enabled.

Examples To view a summary of the security ACLs in the edit buffer, type the following command:

```
PROMPT# show security acl editbuffer
ACL edit-buffer table
```

ACL	Type	Status
acl_111	IP	Not committed
acl-a	IP	Not committed

To view details about these uncommitted ACLs, type the following command.

```
PROMPT# show security acl info all editbuffer
ACL edit-buffer information for all
set security acl ip acl-111 (ACEs 3, add 3, del 0, modified 2)
-----
1. permit IP source IP 192.168.254.12 0.0.0.0 destination IP any
2. permit IP source IP 192.168.253.11 0.0.0.0 destination IP any
3. deny SRC source IP 192.168.253.1 0.0.0.255
set security acl ip acl-a (ACEs 1, add 1, del 0, modified 0)
-----
1. permit SRC source IP 192.168.1.1 0.0.0.0
```

See Also

- 1 **clear security acl** on page 454
- 1 **commit security acl** on page 458
- 1 **set security acl** on page 460
- 1 **show security acl** on page 470

- 1 **show security acl info** on page 473

show security acl hits

Displays the number of packets filtered by security ACLs (“hits”) on the UNIVERGE WL Controller. Each time a packet is filtered by a security ACL, the hit counter increments.

Syntax **show security acl hits**

Defaults None.

Access Enabled.

Usage For UNIVERGE WL Control System to count hits for a security ACL, you must specify **hits** in the **set security acl** commands that define ACE rules for the ACL.

Examples To display the security ACL hits on a UNIVERGE WL Controller, type the following command:

```
PROMPT# show security acl hits
ACL hit-counters
```

Index	Counter	ACL-name
1	0	acl_2
2	0	acl_175
3	916	acl_123

See Also

- 1 **set security acl hit-sample-rate** on page 469
- 1 **set security acl** on page 460

show security acl info

Displays the contents of a specified security ACL or all security ACLs that are committed—saved in the running configuration and nonvolatile storage—or the contents of security ACLs in the edit buffer before they are committed.

Syntax `show security acl info` [*acl-name* | **all**] [**editbuffer**]

<i>acl-name</i>	Name of an existing security ACL to display. ACL names must start with a letter and are case-insensitive.
all	Displays the contents of all security ACLs.
editbuffer	Displays the contents of the specified security ACL or all security ACLs that are stored in the edit buffer after being created with set security acl . If you do not use this parameter, only committed ACLs are shown.

Defaults None.

Access Enabled.

Examples To display the contents of all security ACLs committed on a UNIVERGE WL Controller, type the following command:

```
PROMPT# show security acl info
ACL information for all
set security acl ip acl_123 (hits #5 462)
-----
1. permit IP source IP 192.168.1.11 0.0.0.255 destination IP any enable-hits
2. deny IP source IP 192.168.2.11 0.0.0.0 destination IP any
set security acl ip acl_134 (hits #3 0)
-----
1. permit IP source IP 192.168.0.1 0.0.0.0 destination IP any enable-hits
set security acl ip acl_135 (hits #2 0)
-----
1. deny IP source IP 192.168.1.1 0.0.0.0 destination IP any enable-hits
```

The following command displays the contents of *acl_123* in the edit buffer, including the committed ACE rules 1 and 2 and the uncommitted rule 3:

```
PROMPT# show security acl info acl_123 editbuffer
ACL edit-buffer information for acl_123
```

show security acl map

Chapter 14

```
set security acl ip acl_123 (ACEs 3, add 3, del 0, modified 0)
-----
1. permit IP source IP 192.168.1.11 0.0.0.255 destination IP any enable-hits
2. deny IP source IP 192.168.2.11 0.0.0.0 destination IP any
3. deny SRC source IP 192.168.1.234 255.255.255.255 enable-hits
```

See Also

- 1 **clear security acl** on page 454
- 1 **commit security acl** on page 458
- 1 **set security acl** on page 460

show security acl map

Displays the VLANs, ports, and virtual ports on the UNIVERGE WL Controller to which a security ACL is assigned.

Syntax **show security acl map** *acl-name*

<i>acl-name</i>	Name of an existing security ACL for which to show static mapping. ACL names must start with a letter and are case-insensitive.
-----------------	---

Defaults None.

Access Enabled.

Examples The following command displays the port to which security ACL *acl_111* is mapped:

```
PROMPT# show security acl map acl_111
ACL acl_111 is mapped to:
ap 4 in
```

See Also

- 1 **clear security acl map** on page 456
- 1 **set security acl map** on page 467
- 1 **show security acl** on page 470

show security acl resource-usage

Displays statistics about the resources used by security ACL filtering on the UNIVERGE WL Controller.

Syntax `show security acl resource-usage`

Defaults None.

Access Enabled.

Usage Use this command with the help of the UNIVERGE WL Control System to diagnose an ACL resource problem.

Examples To display security ACL resource usage, type the following command:

```
PROMPT# show security acl resource-usage
ACL resources
```

```
Classifier tree counters
```

```
-----
Number of rules           : 2
Number of leaf nodes      : 1
Stored rule count         : 2
Leaf chain count          : 1
Longest leaf chain        : 2
Number of non-leaf nodes  : 0
Uncompressed Rule Count   : 2
Maximum node depth        : 1
Sub-chain count           : 0
PSCBs in primary memory   : 0 (max: 512)
PSCBs in secondary memory : 0 (max: 9728)
Leaves in primary         : 2 (max: 151)
Leaves in secondary       : 0 (max: 12096)
Sum node depth            : 1
```

```
Information on Network Processor status
```

```
-----
Fragmentation control     : 0
UC switchdest             : 0
```

```
ACL resources
```

```
Port number               : 0
Number of action types     : 2
LUdef in use              : 5
Default action pointer     : c8007dc
L4 global                  : True
No rules                   : False
Non-IP rules               : False
Root in first              : True
```

show security acl resource-usage

Chapter 14

```
Static default action      : False
No per-user (MAC) mapping : True
Out mapping                : False
In mapping                 : True
No VLAN or PORT mapping   : False
No VPORT mapping          : True
```

Table 58 explains the fields in the **show security acl resource-usage** output.

Table 58. show security acl resource-usage Output

Field	Description
Number of rules	Number of security ACEs currently mapped to ports or VLANs.
Number of leaf nodes	Number of security ACL data entries stored in the rule tree.
Stored rule count	Number of security ACEs stored in the rule tree.
Leaf chain count	Number of chained security ACL data entries stored in the rule tree.
Longest leaf chain	Longest chain of security ACL data entries stored in the rule tree.
Number of non-leaf nodes	Number of nodes with no data entries stored in the rule tree.
Uncompressed Rule Count	Number of security ACEs stored in the rule tree, including duplicates—ACEs in ACLs applied to multiple ports, virtual ports, or VLANs.
Maximum node depth	Number of data elements in the rule tree, from the root to the furthest data entry (leaf).
Sub-chain count	Sum of action types represented in all security ACL data entries.
PSCBs in primary memory	Number of pattern search control blocks (PSCBs) stored in primary node memory.
PSCBs in secondary memory	Number of PSCBs stored in secondary node memory.
Leaves in primary	Number of security ACL data entries stored in primary leaf memory.

Table 58. show security acl resource-usage Output

Field	Description
Leaves in secondary	Number of ACL data entries stored in secondary leaf memory.
Sum node depth	Total number of security ACL data entries.
Fragmentation control	Control value for handling fragmented IP packets. Note: The UNIVERGE WL Control System filters only the first packet of a fragmented IP packet and passes the remaining fragments.
UC switchdest	Control value for handling fragmented IP packets. Note: The UNIVERGE WL Control System filters only the first packet of a fragmented IP packet and passes the remaining fragments.
Port number	Control value for handling fragmented IP packets. Note: The UNIVERGE WL Control System filters only the first packet of a fragmented IP packet and passes the remaining fragments.
Number of action types	Number of actions that can be performed by ACLs. This value is always 2, because ACLs can either <i>permit</i> or <i>deny</i> .
LUdef in use	Number of the lookup definition (LUdef) table currently in use for packet handling.
Default action pointer	Memory address used for packet handling, from which default action data is obtained when necessary.
L4 global	Security ACL mapping on the UNIVERGE WL Controller: <ul style="list-style-type: none"> • True—Security ACLs are mapped. • False—No security ACLs are mapped.
No rules	Security ACE rule mapping on the UNIVERGE WL Controller: <ul style="list-style-type: none"> • True—No security ACEs are mapped. • False—Security ACEs are mapped.

Table 58. show security acl resource-usage Output

Field	Description
Non-IP rules	<p>Non-IP security ACE mapping on the UNIVERGE WL Controller:</p> <ul style="list-style-type: none"> • True—Non-IP security ACEs are mapped. • False—Only IP security ACEs are mapped. <p>Note: UNIVERGE WL Control System supports security ACEs for IP only.</p>
Root in first	<p>Leaf buffer allocation:</p> <ul style="list-style-type: none"> • True—Enough primary leaf buffers are allocated in nonvolatile memory to accommodate all leaves. • False—Insufficient primary leaf buffers are allocated in nonvolatile memory to accommodate all leaves.
Static default action	<p>Definition of a default action:</p> <ul style="list-style-type: none"> • True—A default action types is defined. • False—No default action type is defined.
No per-user (MAC) mapping	<p>Per-user application of a security ACL with the Filter-Id attribute, on the UNIVERGE WL Controller:</p> <ul style="list-style-type: none"> • True—No security ACLs are applied to users. • False—Security ACLs are applied to users.
Out mapping	<p>Application of security ACLs to outgoing traffic on the UNIVERGE WL Controller:</p> <ul style="list-style-type: none"> • True—Security ACLs are mapped to outgoing traffic. • False—No security ACLs are mapped to outgoing traffic.
In mapping	<p>Application of security ACLs to incoming traffic on the UNIVERGE WL Controller:</p> <ul style="list-style-type: none"> • True—Security ACLs are mapped to incoming traffic. • False—No security ACLs are mapped to incoming traffic.

Table 58. show security acl resource-usage Output

Field	Description
No VLAN or PORT mapping	Application of security ACLs to UNIVERGE WL Controller VLANs or ports on the UNIVERGE WL Controller: <ul style="list-style-type: none">• True—No security ACLs are mapped to VLANs or ports.• False—Security ACLs are mapped to VLANs or ports.
No VPORT mapping	Application of security ACLs to UNIVERGE WL Controller virtual ports on the UNIVERGE WL Controller: <ul style="list-style-type: none">• True—No security ACLs are mapped to virtual ports.• False—Security ACLs are mapped to virtual ports.

show security acl resource-usage

Chapter 14

Cryptography Commands

A digital certificate is a form of electronic identification for computers. The UNIVERGE WL Controller requires digital certificates to authenticate its communications to UNIVERGE WLMS and WebView, to Web Authentication clients, and to Extensible Authentication Protocol (EAP) clients for which the UNIVERGE WL performs all EAP processing. Certificates can be generated on the UNIVERGE WL or obtained from a certificate authority (CA). Keys contained within the certificates allow the UNIVERGE WL, its servers, and its wireless clients to exchange information secured by encryption.



Note. If the UNIVERGE WL Controller does not already have certificates, The UNIVERGE WL Control System automatically generates the missing ones the first time you boot using UNIVERGE WL Control System. You do not need to install certificates unless you want to replace the ones automatically generated by UNIVERGE WL Control System. (For more information, see the “Certificates Automatically Generated by UNIVERGE WL Control System” section in the “Managing Keys and Certificates” chapter of the [Configuration Guide](#).)



Note. Before installing a new certificate, verify with the **show timedate** and **show timezone** commands that the UNIVERGE WL Controller is set to the correct date, time, and time zone. Otherwise, certificates might not be installed correctly.

This chapter presents cryptography commands alphabetically. Use the following table to locate commands in this chapter based on their use.

Encryption Keys	crypto generate key on page 485
	show crypto key ssh on page 497
PKCS #7 Certificates	crypto generate request on page 486

	crypto ca-certificate on page 482
	show crypto ca-certificate on page 494
	crypto certificate on page 483
	show crypto certificate on page 495
PKCS #12 Certificate	crypto otp on page 491
	crypto pkcs12 on page 492
Self-Signed Certificate	crypto generate self-signed on page 489

crypto ca-certificate

Installs a certificate authority's own PKCS #7 certificate into the UNIVERGE WL Controller certificate and key storage area.

Syntax **crypto ca-certificate** {**admin** | **eap** | **web**} *PEM-formatted-certificate*

admin	Stores the certificate authority's certificate that signed the administrative certificate for the UNIVERGE WL Controller. The administrative certificate authenticates the UNIVERGE WL Controller to UNIVERGE WLMS or WebView.
eap	Stores the certificate authority's certificate that signed the Extensible Authentication Protocol (EAP) certificate for the UNIVERGE WL Controller . The EAP certificate authenticates the UNIVERGE WL Controller to 802.1X supplicants (clients).
web	Stores the certificate authority's certificate that signed the Web Authentication certificate for the UNIVERGE WL Controller . The Web certificate authenticates the UNIVERGE WL Controller to clients who use Web Authentication.
<i>PEM-formatted-certificate</i>	ASCII text representation of the certificate authority PKCS #7 certificate, consisting of up to 5120 characters that you have obtained from the certificate authority.

Defaults None.

Access Enabled.

Usage The Privacy-Enhanced Mail protocol (PEM) format is used for representing a PKCS #7 certificate in ASCII text. PEM uses base64 encoding to convert the certificate to ASCII text, then puts the encoded text between the following delimiters:

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

To use this command, you must already have obtained a copy of the certificate authority's certificate as a PKCS #7 object file. Then do the following:

- 1 Open the PKCS #7 object file with an ASCII text editor such as Notepad or vi.
- 2 Enter the **crypto ca-certificate** command on the CLI command line.
- 3 When UNIVERGE WL Control System prompts you for the PEM-formatted certificate, paste the PKCS #7 object file onto the command line.

Examples The following command adds the certificate authority's certificate to UNIVERGE WL Controller certificate and key storage:

```
UNIVERGE WL Controller# crypto ca-certificate admin
Enter PEM-encoded certificate
-----BEGIN CERTIFICATE-----
MIIDwDCCA2ggAwIBAgIQL2jvuu4P05FAQCyewU3ojANBgkqhkiG9w0BAQUFADCB
mzerMClaweVQQTTooewi\wpoer0QWNFNkj90044mbdr11277SWQ8G7DiwYUtrqoQplKJvxz
.....
Lm8wmVYxP56M;CUAm908C2foYgOY40=
-----END CERTIFICATE-----
```

See Also **show crypto ca-certificate** on page 494

crypto certificate

Installs one of the UNIVERGE WL Controller's PKCS #7 certificates into the certificate and key storage area on the UNIVERGE WL Controller. The certificate, which is issued and signed by a certificate authority, authenticates the UNIVERGE WL Controller either to UNIVERGE WLMS or WebView, or to 802.1X supplicants (clients).

Syntax **crypto certificate** { **admin** | **eap** | **web** } *PEM-formatted certificate*

admin	Stores the certificate authority's administrative certificate, which authenticates the UNIVERGE WL Controller to UNIVERGE WLMS or WebView.
eap	Stores the certificate authority's Extensible Authentication Protocol (EAP) certificate, which authenticates the UNIVERGE WL Controller to 802.1X supplicants (clients).
web	Stores the certificate authority's Web Authentication certificate, which authenticates the UNIVERGE WL Controller to clients who use Web Authentication.
<i>PEM-formatted certificate</i>	ASCII text representation of the PKCS #7 certificate, consisting of up to 5120 characters, that you have obtained from the certificate authority.

Defaults None.

Access Enabled.

Usage To use this command, you must already have generated a certificate request with the **crypto generate request** command, sent the request to the certificate authority, and obtained a signed copy of the UNIVERGE WL Controller certificate as a PKCS #7 object file. Then do the following:

- 1 Open the PKCS #7 object file with an ASCII text editor such as Notepad or vi.
- 2 Enter the **crypto certificate** command on the CLI command line.
- 3 When UNIVERGE WL Control System prompts you for the PEM-formatted certificate, paste the PKCS #7 object file onto the command line.

The UNIVERGE WL Controller verifies the validity of the public key associated with this certificate before installing it, to prevent a mismatch between the UNIVERGE WL Controller's private key and the public key in the installed certificate.

Examples The following command installs a certificate:

```
PROMPT# crypto certificate admin
Enter PEM-encoded certificate
```

```
-----BEGIN CERTIFICATE-----
MIIBdTCP3wIBADA2MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQOEExGjAYBgNVBAMU
EXR1Y2hwdWJzQHRycHouY29tMIGfMAOGCSqGSIb3DQEBAQAA4GNADCBiQKBgQC4
.....
2L8Q9tk+G2As84QYLm8wmVY>xP56M;CUAm908C2foYgOY40=
-----END CERTIFICATE-----
```

See Also

- 1 **crypto generate request** on page 486
- 1 **crypto generate self-signed** on page 489

crypto generate key

Generates an RSA public-private encryption key pair that is required for a Certificate Signing Request (CSR) or a self-signed certificate. For SSH, generates an authentication key.

Syntax **crypto generate key** { **admin** | **domain** | **eap** | **ssh** | **web** }
{ **128** | **512** | **1024** | **2048** }

admin	Generates an administrative key pair for authenticating the UNIVERGE WL Controller to UNIVERGE WLMS or WebView.
domain	Generates a key pair for authenticating management traffic exchanged by UNIVERGE WL Controller within a Mobility Domain.
eap	Generates an EAP key pair for authenticating the UNIVERGE WL Controller to 802.1X supplicants (clients).
ssh	Generates a key pair for authenticating the UNIVERGE WL Controller to Secure Shell (SSH) clients.

crypto generate request

Chapter 15

web Generates an administrative key pair for authenticating the UNIVERGE WL Controller to Web Authentication clients.

128 | 512 | 1024 | 2048 Length of the key pair in bits.

Note: The minimum key length for SSH is **1024**. The length **128** applies only to **domain** and is the only valid option for it.

Defaults None.

Access Enabled.

Usage You can overwrite a key by generating another key of the same type.

SSH requires an SSH authentication key, but you can allow UNIVERGE WL Control System to generate it automatically. The first time an SSH client attempts to access the SSH server on a UNIVERGE WL Controller, the UNIVERGE WL Controller automatically generates a 1024-byte SSH key. If you want to use a 2048-byte key instead, use the **crypto generate key ssh 2048** command to generate one.

Examples To generate an administrative key for use with UNIVERGE WLMS, type the following command:

```
UNIVERGE WL Controller# crypto generate key admin 1024  
key pair generated
```

See Also **show crypto key ssh** on page 497

crypto generate request

Generates a Certificate Signing Request (CSR). This command outputs a PEM-formatted PKCS #10 text string that you can cut and paste to another location for delivery to a certificate authority.

This command generates either an administrative CSR for use with UNIVERGE WLMS and WebView, or an EAP CSR for use with 802.1X clients.

Syntax `crypto generate request { admin | eap | web }`

admin	Generates a request for an administrative certificate to authenticate the UNIVERGE WL Controller to UNIVERGE WLMS or WebView.
eap	Generates a request for an EAP certificate to authenticate the UNIVERGE WL Controller to 802.1X supplicants (clients).
web	Generates a request for a Web Authentication certificate to authenticate the UNIVERGE WL Controller to Web Authentication clients.

After type the command, you are prompted for the following variables:

Country Name <i>string</i>	(Optional) Specify the abbreviation for the country in which the UNIVERGE WL Controller is operating, in 2 alphanumeric characters with no spaces.
State Name <i>string</i>	(Optional) Specify the name of the state, in up to 64 alphanumeric characters. Spaces are allowed.
Locality Name <i>string</i>	(Optional) Specify the name of the locality, in up to 80 alphanumeric characters with no spaces.
Organizational Name <i>string</i>	(Optional) Specify the name of the organization, in up to 80 alphanumeric characters with no spaces.
Organizational Unit <i>string</i>	(Optional) Specify the name of the organizational unit, in up to 80 alphanumeric characters with no spaces.
Common Name <i>string</i>	Specify a unique name for the UNIVERGE WL Controller, in up to 80 alphanumeric characters with no spaces. Use a fully qualified name if such names are supported on your network. This field is required.
Email Address <i>string</i>	(Optional) Specify your email address, in up to 80 alphanumeric characters with no spaces.
Unstructured Name <i>string</i>	(Optional) Specify any name, in up to 80 alphanumeric characters with no spaces.

Defaults None.

crypto generate request

Chapter 15

Access Enabled.

Usage To use this command, you must already have generated a public-private encryption key pair with the **crypto generate key** command.

Enter **crypto generate request admin**, **crypto generate request eap**, or **crypto generate request web** and press Enter. When you are prompted, type the identifying values in the fields, or press Enter if the field is optional. You must enter a common name for the UNIVERGE WL Controller.

This command outputs a PKCS #10 text string in Privacy-Enhanced Mail protocol (PEM) format that you paste to another location for submission to the certificate authority. You then send the request to the certificate authority to obtain a signed copy of the UNIVERGE WL Controller certificate as a PKCS #7 object file.

Examples To request an administrative certificate from a certificate authority, type the following command:

```
PROMPT# crypto generate request admin
Country Name: US
State Name: CA
Locality Name: Pleasanton
Organizational Name: UNIVERGE
Organizational Unit: ENG
Common Name: ENG
Email Address: admin@example.com
Unstructured Name: admin
CSR for admin is
-----BEGIN CERTIFICATE REQUEST-----
MIIBuzCCASQCAQAwEzELMAkGA1UEBhMCdXMxCzAJBgNVBAGTAzAmNhMQswCQYDVQQL
EwJjYU9wOBAQEFAAOBjQAwgYkCgYEA1zatpYSt0jHMa0QJmWHeZPPFGQ9kBEimJKPG
bznFjAC780GcZtnJPGqnMnOKj/4NdKnonT6NdCd2fBdGbuEFGNMNgZMYKGcV2JIu
tr*P*z*exECscaNlicKMYa$$LQo621vh67RM1KTMECM6uCB6XNypIHn1gtrrpL/
LhyGTUcAwEAAaAAMA0GCSqGSIb3DQEBAUAA4GBAHK5z2kfjBbV/F0b0MyC5S7K
htsw7T4SwmCi j55qfUHxsRelggYcw6vJtr57jJ7wFfsMd8C50NcbJLFlNYC9OKkB
hW+5gDPA0Zd0nnr591XKz3Zzyvyrktv00rcld8Fo2RtTQ3AOT9cUZqJVel085GXJ
-----END CERTIFICATE REQUEST-----
```

See Also

- 1 **crypto certificate** on page 483
- 1 **crypto generate key** on page 485

crypto generate self-signed

Generates a self-signed certificate for either an administrative certificate for use with UNIVERGE WLMS or an EAP certificate for use with 802.1X wireless users.

Syntax `crypto generate self-signed {admin | eap | web}`

admin	Generates an administrative certificate to authenticate the UNIVERGE WL Controller to UNIVERGE WLMS or WebView.
eap	Generates an EAP certificate to authenticate the UNIVERGE WL Controller to 802.1X supplicants (clients).
web	Generates a Web Authentication certificate to authenticate the UNIVERGE WL Controller to Web Authentication clients.

After type the command, you are prompted for the following variables:

Country Name <i>string</i>	(Optional) Specify the abbreviation for the country in which the UNIVERGE WL Controller is operating, in 2 alphanumeric characters with no spaces.
State Name <i>string</i>	(Optional) Specify the abbreviation for the name of the state, in 2 alphanumeric characters with no spaces.
Locality Name <i>string</i>	(Optional) Specify the name of the locality, in up to 80 alphanumeric characters with no spaces.
Organizational Name <i>string</i>	(Optional) Specify the name of the organization, in up to 80 alphanumeric characters with no spaces.
Organizational Unit <i>string</i>	(Optional) Specify the name of the organizational unit, in up to 80 alphanumeric characters with no spaces.

crypto generate self-signed

Chapter 15

Common Name Specify a unique name for the UNIVERGE WL Controller, in up to 80 alphanumeric characters with no spaces. Use a fully qualified name if such names are supported on your network. This field is required.
string

Note: If you are generating a Web Authentication (**web**) certificate, use a common name that looks like a domain name (two or more strings connected by dots, with no spaces). For example, use *common.name* instead of *common name*. The string is not required to be an actual domain name. It simply needs to be formatted like one.

Email Address (Optional) Specify your email address, in up to 80 alphanumeric characters with no spaces.
string

Unstructured Name (Optional) Specify any name, in up to 80 alphanumeric characters with no spaces.
string

Defaults None.

Access Enabled.

Usage To use this command, you must already have generated a public-private encryption key pair with the **crypto generate key** command.

Examples To generate a self-signed administrative certificate, type the following command:

```
PROMPT# crypto generate self-signed admin
Country Name:
State Name:
Locality Name:
Organizational Name:
Organizational Unit:
Common Name: wl@example.com
Email Address:
Unstructured Name:
success: self-signed cert for admin generated
```

See Also

- 1 **crypto certificate** on page 483
- 1 **crypto generate key** on page 485

crypto otp

Sets a one-time password (OTP) for use with the **crypto pkcs12** command.

Syntax **crypto otp** {**admin** | **eap** | **web**} *one-time-password*

admin Creates a one-time password for installing a PKCS #12 object file for an administrative certificate and key pair—and optionally the certificate authority's own certificate—to authenticate the UNIVERGE WL Controller to UNIVERGE WLMS or WebView.

eap Creates a one-time password for installing a PKCS #12 object file for an EAP certificate and key pair—and optionally the certificate authority's own certificate—to authenticate the UNIVERGE WL Controller to 802.1X supplicants (clients).

web Creates a one-time password for installing a PKCS #12 object file for a Web Authentication certificate and key pair—and optionally the certificate authority's own certificate—to authenticate the UNIVERGE WL Controller to Web Authentication clients.

one-time-password Password of at least 1 alphanumeric character, with no spaces, for clients other than Microsoft Windows clients. The password must be the same as the password protecting the PKCS #12 object file.

Note: On a UNIVERGE WL Controller that handles communications to and from Microsoft Windows clients, use a one-time password of 31 characters or fewer.

The following characters *cannot* be used as part of the one-time password of a PKCS #12 file:

- Quotation marks (“ ”)
- Question mark (?)
- Ampersand (&)

Defaults None.

Access Enabled.

Usage The password allows the public-private key pair and certificate to be installed together from the same PKCS #12 object file. UNIVERGE WL Control System erases the one-time password after processing the **crypto pkcs12** command or when you reboot the UNIVERGE WL Controller.

UNIVERGE WL Control System recommends that you create a password that is memorable to you but is not subject to easy guesses or a dictionary attack. For best results, create a password of alphanumeric uppercase and lowercase characters.

Examples The following command creates the one-time password *hap9iN#ss* for installing an EAP certificate and key pair:

```
PROMPT# crypto generate otp eap hap9iN#ss
OTP set
```

See Also **crypto pkcs12** on page 492

crypto pkcs12

Unpacks a PKCS #12 object file into the certificate and key storage area on the UNIVERGE WL Controller. This object file contains a public-private key pair, a UNIVERGE WL Controller certificate signed by a certificate authority, and the certificate authority's certificate.

Syntax **crypto pkcs12** {**admin** | **eap** | **web**} *file-location-url*

admin	Unpacks a PKCS #12 object file for an administrative certificate and key pair—and optionally the certificate authority's own certificate—for authenticating the UNIVERGE WL Controller to UNIVERGE WLMS or WebView.
eap	Unpacks a PKCS #12 object file for an EAP certificate and key pair—and optionally the certificate authority's own certificate—for authenticating the UNIVERGE WL Controller to 802.1X supplicants (clients).

web	Unpacks a PKCS #12 object file for a Web Authentication certificate and key pair—and optionally the certificate authority's own certificate—for authenticating the UNIVERGE WL Controller to Web Authentication clients.
<i>file-location-url</i>	Location of the PKCS #12 object file to be installed. Specify a location of between 1 and 128 alphanumeric characters, with no spaces.

Defaults The password you enter with the **crypto otp** command must be the same as the one protecting the PKCS #12 file.

Access Enabled.

Usage To use this command, you must have already created a one-time password with the **crypto otp** command.

You must also have the PKCS #12 object file available. You can download a PKCS #12 object file via TFTP from a remote location to the local nonvolatile storage system on the UNIVERGE WL Controller.

Examples The following commands copy a PKCS #12 object file for an EAP certificate and key pair—and optionally the certificate authority's own certificate—from a TFTP server to nonvolatile storage on the UNIVERGE WL Controller, create the one-time password *hap9iN#ss*, and unpack the PKCS #12 file:

```
PROMPT# copy tftp://192.168.253.1/2048full.p12 2048full.p12
success: received 637 bytes in 0.253 seconds [ 2517 bytes/sec]
```

```
PROMPT# crypto otp eap hap9iN#ss
OTP set
```

```
PROMPT# crypto pkcs12 eap 2048full.p12
Unwrapped from PKCS12 file:
    keypair
    device certificate
    CA certificate
```

See Also **crypto otp** on page 491

show crypto ca-certificate

Displays information about the certificate authority's PEM-encoded PKCS #7 certificate.

Syntax **show crypto ca-certificate** {**admin** | **eap** | **web**}

admin Displays information about the certificate authority's certificate that signed the administrative certificate for the UNIVERGE WL Controller.

The administrative certificate authenticates the UNIVERGE WL Controller to UNIVERGE WLMS or WebView.

eap Displays information about the certificate authority's certificate that signed the Extensible Authentication Protocol (EAP) certificate for the UNIVERGE WL Controller.

The EAP certificate authenticates the UNIVERGE WL Controller to 802.1X supplicants (clients).

web Displays information about the certificate authority's certificate that signed the Web Authentication certificate for the UNIVERGE WL Controller.

The Web Authentication certificate authenticates the UNIVERGE WL Controller to Web Authentication clients.

Defaults None.

Access Enabled.

Examples To display information about the certificate of a certificate authority, type the following command:

PROMPT# **show crypto ca-certificate**

Table 59 describes the fields in the display.

Table 59. show crypto ca-certificate Output

Fields	Description
Version	Version of the X.509 certificate.
Serial Number	A unique identifier for the certificate or signature.
Subject	Name of the certificate owner.
Signature Algorithm	Algorithm that created the signature, such as RSA MD5 or RSA SHA.
Issuer	Certificate authority that issued the certificate or signature.
Validity	Time period for which the certificate is valid.

See Also

- 1 **crypto ca-certificate** on page 482
- 1 **show crypto certificate** on page 495

show crypto certificate

Displays information about one of the cryptographic certificates installed on the UNIVERGE WL Controller.

Syntax **show crypto certificate** {**admin** | **eap** | **web**}

admin	Displays information about the administrative certificate that authenticates the UNIVERGE WL Controller to UNIVERGE WLMS or WebView.
eap	Displays information about the EAP certificate that authenticates the UNIVERGE WL Controller to 802.1X supplicants (clients).
web	Displays information about the Web Authentication certificate that authenticates the UNIVERGE WL Controller to Web Authentication clients.

Defaults **None.**

show crypto certificate

Chapter 15

Access Enabled.

Usage You must have generated a self-signed certificate or obtained a certificate from a certificate authority before displaying information about the certificate.

Examples To display information about a cryptographic certificate, type the following command:

```
PROMPT# show crypto certificate eap
```

Table 60 describes the fields of the display.

Table 60. crypto certificate Output

Fields	Description
Version	Version of the X.509 certificate.
Serial Number	A unique identifier for the certificate or signature.
Subject	Name of the certificate owner.
Signature Algorithm	Algorithm that created the signature, such as RSA MD5 or RSA SHA.
Issuer	Certificate authority that issued the certificate or signature.
Validity	Time period for which the certificate is valid.

See Also

- 1 **crypto generate self-signed** on page 489
- 1 **show crypto ca-certificate** on page 494

show crypto key ssh

Displays SSH authentication key information. This command displays the checksum (also called a *fingerprint*) of the public key. When you connect to the UNIVERGE WL Controller with an SSH client, you can compare the SSH key checksum displayed by the UNIVERGE WL Controller with the one displayed by the client to verify that you really are connected to the UNIVERGE WL Controller and not another device. Generally, SSH clients remember the encryption key after the first connection, so you need to check the key only once.

Syntax `show crypto key ssh`

Defaults None.

Access Enabled.

Examples To display SSH key information, type the following command:

```
PROMPT# show crypto key ssh  
ec:6f:56:7f:d1:fd:c0:28:93:ae:a4:f9:7c:f5:13:04
```

See Also `crypto generate key` on page 485

show crypto key ssh
Chapter 15

RADIUS and Server Groups Commands

Use RADIUS commands to set up communication between a UNIVERGE WL Controller and groups of up to four RADIUS servers for remote authentication, authorization, and accounting (AAA) of administrators and network users. This chapter presents RADIUS commands alphabetically. Use the following table to locate commands in this chapter based on their uses.

RADIUS Client	set radius client system-ip on page 506
	clear radius client system-ip on page 501
RADIUS Servers	set radius on page 503
	set radius server on page 506
	clear radius on page 500
	clear radius server on page 502
Server Groups	set server group on page 509
	set server group load-balance on page 510
	clear server group on page 502

(For information about RADIUS attributes, see the RADIUS appendix in the [Configuration Guide](#).)

clear radius

Resets parameters that were globally configured for RADIUS servers to their default values.

Syntax `clear radius { deadtime | key | retransmit | timeout }`

deadtime	Number of minutes to wait after declaring an unresponsive RADIUS server unavailable before retrying the RADIUS server.
key	Password (shared secret key) used to authenticate to the RADIUS server.
retransmit	Number of transmission attempts made before declaring an unresponsive RADIUS server unavailable.
timeout	Number of seconds to wait for the RADIUS server to respond before retransmitting.

Defaults Global RADIUS parameters have the following default values:

- 1 **deadtime**—0 (zero) minutes (The UNIVERGE WL Controller does not designate unresponsive RADIUS servers as unavailable.)
- 1 **key**—No key
- 1 **retransmit**—3 (the total number of attempts, including the first attempt)
- 1 **timeout**—5 seconds

Access Enabled.

Usage To override the globally set values on a particular RADIUS server, use the **set radius server** command.

Examples To reset all global RADIUS parameters to their factory defaults, type the following commands:

```
PROMPT# clear radius deadtime
success: change accepted.

PROMPT# clear radius key
success: change accepted.

PROMPT# clear radius retransmit
```

success: change accepted.

PROMPT# clear radius timeout

success: change accepted.

See Also

- 1 **set radius** on page 503
- 1 **set radius server** on page 506
- 1 **show aaa** on page 240

clear radius client system-ip

Removes the UNIVERGE WL Controllers system IP address from use as the permanent source address in RADIUS client requests from the UNIVERGE WL Controller to its RADIUS server(s).

Syntax clear radius client system-ip

Defaults None.

Access Enabled.

Usage The **clear radius client system-ip** command causes the UNIVERGE WL Controller to use the IP address of the interface through which it sends a RADIUS client request as the source IP address. The UNIVERGE WL Controller selects a source interface address based on information in its routing table as the source address for RADIUS packets leaving the UNIVERGE WL Controller.

Examples To clear the system IP address as the permanent source address for RADIUS client requests, type the following command:

PROMPT# clear radius client system-ip

success: change accepted.

See Also

- 1 **set radius client system-ip** on page 506
- 1 **show aaa** on page 240

clear radius server

Removes the named RADIUS server from the UNIVERGE WL Controller configuration.

Syntax **clear radius server** *server-name*

server-name Name of a RADIUS server configured to perform remote AAA services for the UNIVERGE WL Controller.

Defaults None.

Access Enabled.

Examples The following command removes the RADIUS server *rs42* from a list of remote AAA servers:

```
PROMPT# clear radius server rs42
success: change accepted.
```

See Also

- 1 **set radius server** on page 506
- 1 **show aaa** on page 240

clear server group

Removes a RADIUS server group from the configuration, or disables load balancing for the group.

Syntax **clear server group** *group-name* [**load-balance**]

group-name Name of a RADIUS server group configured to perform remote AAA services for UNIVERGE WL Controllers.

load-balance Ability of group members to share demand for services among servers.

Defaults None.

Access Enabled.

Usage Deleting a server group removes the server group from the configuration. However, the members of the server group remain.

Examples To remove the server group *sg-77* type the following command:

```
PROMPT# clear server group sg-77
success: change accepted.
```

To disable load balancing in a server group *shorebirds*, type the following command:

```
PROMPT# set server group shorebirds load-balance disable
success: change accepted.
```

See Also **set server group** on page 509

set radius

Configures global defaults for RADIUS servers that do not explicitly set these values themselves. By default, the UNIVERGE WL Controller automatically sets all these values except the password (key).

Syntax **set radius** { **deadtime** *minutes* | **encrypted-key** *string* | **key** *string* | **retransmit** *number* | **timeout** *seconds* }

deadtime *minutes*

Number of minutes the UNIVERGE WL Controller waits after declaring an unresponsive RADIUS server unavailable before retrying the RADIUS server. You can specify from 0 to 1440 minutes.

encrypted-key *string*

Password (shared secret key) used to authenticate to the RADIUS server, entered in its encrypted form. You must provide the same encrypted password that is defined on the RADIUS server. The password can be 1 to 64 characters long, with no spaces or tabs.

UNIVERGE WL Control Systemr does not encrypt the string you enter, and instead displays the string in **show config** and **show aaa** output exactly as you entered it.

Note: Use this option only if you are entering the key in its encrypted form. To enter the key in unencrypted form, use the **key string** option instead.

key *string*

Password (shared secret key) used to authenticate to the RADIUS server, entered in its unencrypted form. You must provide the same password that is defined on the RADIUS server. The password can be 1 to 64 characters long, with no spaces or tabs.

UNIVERGE WL Control Systemr encrypts the displayed form of the string in **show config** and **show aaa** output.

Note: Use this option only if you are entering the key in its unencrypted form. To enter the key in encrypted form, use the **encrypted-key string** option instead.

retransmit <i>number</i>	Number of transmission attempts the UNIVERGE WL Controller makes before declaring an unresponsive RADIUS server unavailable. You can specify from 1 to 100 retries.
timeout <i>seconds</i>	Number of seconds the UNIVERGE WL Controller waits for the RADIUS server to respond before retransmitting. You can specify from 1 to 65,535.

Defaults Global RADIUS parameters have the following default values:

- 1 **deadtime**—0 (zero) minutes (The UNIVERGE WL Controller does not designate unresponsive RADIUS servers as unavailable.)
- 1 **encrypted-key**—No key
- 1 **key**—No key
- 1 **retransmit**—3 (the total number of attempts, including the first attempt)
- 1 **timeout**—5 seconds

Access Enabled.

Usage You can specify only one parameter per command line.

Examples The following commands sets the dead time to 5 minutes, the RADIUS key to *goody*, the number of retransmissions to 1, and the timeout to 21 seconds on all RADIUS servers connected to the UNIVERGE WL Controller:

```
Controller# set radius deadtime 5
success: change accepted.

Controller# set radius key goody
success: change accepted.

Controller# set radius retransmit 1
success: change accepted.

Controller# set radius timeout 21
success: change accepted.
```

See Also

- 1 **clear radius server** on page 502
- 1 **set radius server** on page 506
- 1 **show aaa** on page 240

set radius client system-ip

Causes all RADIUS requests to be sourced from the IP address specified by the **set system ip-address** command, providing a permanent source IP address for RADIUS packets sent from the UNIVERGE WL Controller.

Syntax **set radius client system-ip**

Defaults None. If you do not use this command, RADIUS packets leaving the UNIVERGE WL Controller have the source IP address of the outbound interface, which can change as routing conditions change.

Access Enabled.

Usage The UNIVERGE WL Controller system IP address must be set before you use this command.

Examples The following command sets the UNIVERGE WL Controller system IP address as the address of the RADIUS client:

```
PROMPT# set radius client system-ip
success: change accepted.
```

See Also

- 1 **clear radius client system-ip** on page 501
- 1 **set system ip-address** on page 36

set radius server

Configures RADIUS servers and their parameters. By default, the UNIVERGE WL Controller automatically sets all these values except the password (key).

Syntax **set radius server** *server-name* [**address** *ip-address*] [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *number*] [**deadtime** *minutes*] [[**key** *string*] | [**encrypted-key** *string*]] [**author-password** *password*]

<i>server-name</i>	Unique name for this RADIUS server. Enter an alphanumeric string of up to 32 characters, with no blanks.
--------------------	--

address <i>ip-address</i>	IP address of the RADIUS server. Enter the address in dotted decimal notation.
auth-port <i>port-number</i>	UDP port that the UNIVERGE WL Controller uses for authentication and authorization.
acct-port <i>port-number</i>	UDP port that the UNIVERGE WL Controller uses for accounting.
timeout <i>seconds</i>	Number of seconds the UNIVERGE WL Controller waits for the RADIUS server to respond before retransmitting. You can specify from 1 to 65,535 seconds.
retransmit <i>number</i>	Number of transmission attempts made before declaring an unresponsive RADIUS server unavailable. You can specify from 1 to 100 retries.
deadtime <i>minutes</i>	Number of minutes the UNIVERGE WL Controller waits after declaring an unresponsive RADIUS server unavailable before retrying that RADIUS server. Specify between 0 (zero) and 1440 minutes (24 hours). A zero value causes the UNIVERGE WL Controller to identify unresponsive servers as available.
key <i>string</i> / encrypted-key <i>string</i>	<p>Password (shared secret key) the UNIVERGE WL Controller uses to authenticate to RADIUS servers. You must provide the same password that is defined on the RADIUS server. The password can be 1 to 64 characters long, with no spaces or tabs.</p> <ul style="list-style-type: none"> • Use the key option to enter the string in its unencrypted form. UNIVERGE WL Control Systemr encrypts the displayed form of the string in show config and show aaa output. • To enter the string in its encrypted form instead, use the encrypted-key option. UNIVERGE WL Control Systemr does not encrypt the string you enter, and instead displays the string exactly as you enter it.
author-password <i>password</i>	Password used for authorization to a RADIUS server for MAC authentication. The client's MAC address is sent as the username and the author-password string is sent as the password. Specify a password of up to 32 alphanumeric characters with no spaces or tabs.

Defaults Default values are listed below:

set radius server

Chapter 16

- 1 **auth-port**—UDP port 1812
- 1 **acct-port**—UDP port 1813
- 1 **timeout**—5 seconds
- 1 **retransmit**—3 (the total number of attempts, including the first attempt)
- 1 **deadtime**—0 (zero) minutes (The UNIVERGE WL Controller does not designate unresponsive RADIUS servers as unavailable.)
- 1 **key**—No key
- 1 **encrypted-key**—No key
- 1 **author-password**—No Password

Access Enabled.

Usage For a given RADIUS server, the first instance of this command must set both the server name and the IP address and can include any or all of the other optional parameters. Subsequent instances of this command can be used to set optional parameters for a given RADIUS server.

To configure the server as a remote authenticator for the UNIVERGE WL Controller, you must add it to a server group with the **set server group** command.

Do not use the same name for a RADIUS server and a RADIUS server group.

Examples To set a RADIUS server named RS42 with IP address 198.162.1.1 to use the default accounting and authorization ports with a timeout interval of 30 seconds, two transmit attempts, 5 minutes of dead time, and the key string of *keys4u*, type the following command:

```
Controller# set radius server RS42 address 198.162.1.1 timeout 30 retransmit 2  
deadtime 5 key keys4U
```

See Also

- 1 **set authentication admin** on page 203
- 1 **set authentication console** on page 206
- 1 **set authentication dot1x** on page 209
- 1 **set authentication mac** on page 213
- 1 **set authentication web** on page 215

- 1 **set radius** on page 503
- 1 **set server group** on page 509
- 1 **show aaa** on page 240

set server group

Configures a group of one to four RADIUS servers.

Syntax **set server group** *group-name* **members** *server-name1* [*server-name2*] [*server-name3*] [*server-name4*]

group-name Server group name of up to 32 characters, with no spaces or tabs.

members The names of one or more configured RADIUS servers.
server-name1 You can enter up to four server names.

server-name2

server-name3

server-name4

Defaults None.

Access Enabled.

Usage You must assign all group members simultaneously, as shown in the example. To enable load balancing, use **set server group load-balance enable**.

Do not use the same name for a RADIUS server and a RADIUS server group.

Examples To set server group *shorebirds* with members *heron*, *egret*, and *sandpiper*, type the following command:

```
Controller# set server group shorebirds members heron egret sandpiper
success: change accepted.
```

See Also

- 1 **clear server group** on page 502
- 1 **set server group load-balance** on page 510

1 **show aaa** on page 240

set server group load-balance

Enables or disables load balancing among the RADIUS servers in a server group.

Syntax **set server group** *group-name* **load-balance** { **enable** | **disable** }

group-name Server group name of up to 32 characters.

load-balance Enables or disables load balancing of authentication requests among the servers in the group.
enable | **disable**

Defaults Load balancing is disabled by default.

Access Enabled.

Usage You can optionally enable load balancing after assigning the server group members. If you configure load balancing, UNIVERGE WL Control Systemr sends each AAA request to a separate server, starting with the first one on the list and skipping unresponsive servers. If no server in the group responds, UNIVERGE WL Control Systemr moves to the next method configured with **set authentication** and **set accounting**.

In contrast, if load balancing is *not* configured, UNIVERGE WL Control Systemr always begins with the first server in the list and sends unfulfilled requests to each subsequent server in the group before moving on to the next configured AAA method.

Examples To enable load balancing between the members of server group *shorebirds*, type the following command:

```
Controller# set server group shorebirds load-balance enable
success: change accepted.
```

To disable load balancing between *shorebirds* server group members, type the following command:

```
Controller# set server group shorebirds load-balance disable
success: change accepted.
```

See Also

- 1 **clear server group** on page 502
- 1 **clear radius server** on page 502
- 1 **set server group** on page 509
- 1 **show aaa** on page 240

set server group load-balance

Chapter 16

802.1X Management Commands

Use 802.1X management commands to modify the default settings for IEEE 802.1X sessions on a UNIVERGE WL Controller. For best results, change the settings only if you are aware of a problem with 802.1X performance on the UNIVERGE WL Controllers.

This chapter presents 802.1X commands alphabetically. Use the following table to locate commands in this chapter based on their use. For information about configuring 802.1X commands for user authentication, see Chapter 9, “AAA Commands,” on page 183.



Caution! 802.1X parameter settings are global for all SSIDs configured on the UNIVERGE WL Controller.

Keys	set dot1x bonded-period on page 518
	set dot1x key-tx on page 519
	set dot1x tx-period on page 524
	clear dot1x tx-period on page 518
	set dot1x wep-rekey on page 525
Bonded Authentication	set dot1x wep-rekey-period on page 526
	clear dot1x bonded-period on page 514
	set dot1x bonded-period on page 518
Reauthentication	set dot1x reauth on page 521
	set dot1x reauth-max on page 522
	clear dot1x reauth-max on page 516

clear dot1x bonded-period

Chapter 17

	set dot1x reauth-period on page 522
	clear dot1x reauth-period on page 516
Retransmission	set dot1x max-req on page 520
	clear dot1x max-req on page 515
Quiet Period and Timeouts	set dot1x quiet-period on page 520
	clear dot1x quiet-period on page 515
	set dot1x timeout auth-server on page 523
	clear dot1x timeout auth-server on page 517
	set dot1x timeout supplicant on page 524
	clear dot1x timeout supplicant on page 517
Settings, Active Clients, and Statistics	show dot1x on page 526

clear dot1x bonded-period

Resets the Bonded Auth period to its default value.

Syntax **clear dot1x max-req**

Defaults The default bonded authentication period is 0 seconds.

Access Enabled.

Usage

Examples To reset the Bonded period to its default, type the following command:

```
PROMPT# clear dot1x bonded-period
success: change accepted.
```

See Also

1 **set dot1x bonded-period** on page 518

1 **show dot1x** on page 526

clear dot1x max-req

Resets to the default setting the number of Extensible Authentication Protocol (EAP) requests that the UNIVERGE WL Controller retransmits to a supplicant (client).

Syntax clear dot1x max-req

Defaults The default number is 20.

Access Enabled.

Examples To reset the number of 802.1X requests the UNIVERGE WL Controller can send to the default setting, type the following command:

```
PROMPT# clear dot1x max-req
success: change accepted.
```

See Also

1 set dot1x max-req on page 520

1 show dot1x on page 526

clear dot1x quiet-period

Resets the quiet period after a failed authentication to the default setting.

Syntax clear dot1x quiet-period

Defaults The default is 60 seconds.

Access Enabled.

Examples Type the following command to reset the 802.1X quiet period to the default:

```
PROMPT# clear dot1x quiet-period
success: change accepted.
```

See Also

1 set dot1x quiet-period on page 520

1 show dot1x on page 526

clear dot1x reauth-max

Resets the maximum number of reauthorization attempts to the default setting.

Syntax **clear dot1x reauth-max**

Defaults The default is 2 attempts.

Access Enabled.

Examples Type the following command to reset the maximum number of reauthorization attempts to the default:

```
PROMPT# clear dot1x reauth-max
success: change accepted.
```

See Also

1 **set dot1x reauth-max** on page 522

1 **show dot1x** on page 526

clear dot1x reauth-period

Resets the time period that must elapse before a reauthentication attempt, to the default time period.

Syntax **clear dot1x reauth-period**

Defaults The default is 3600 seconds (1 hour).

Access Enabled.

Examples Type the following command to reset the default reauthentication time period:

```
PROMPT# clear dot1x reauth-period
success: change accepted.
```

See Also

1 **set dot1x reauth-period** on page 522

1 **show dot1x** on page 526

clear dot1x timeout auth-server

Resets to the default setting the number of seconds that must elapse before the UNIVERGE WL Controller times out a request to a RADIUS server.

Syntax clear dot1x timeout auth-server

Defaults The default is 30 seconds.

Access Enabled.

Examples To reset the default timeout for requests to an authentication server, type the following command:

```
PROMPT# clear dot1x timeout auth-server
success: change accepted.
```

See Also

1 **set dot1x timeout auth-server** on page 523

1 **show dot1x** on page 526

clear dot1x timeout supplicant

Resets to the default setting the number of seconds that must elapse before the UNIVERGE WL Controller times out an authentication session with a supplicant (client).

Syntax clear dot1x timeout supplicant

Defaults The default for the authentication timeout sessions is 30 seconds.

Access Enabled.

Examples Type the following command to reset the timeout period for an authentication session:

```
PROMPT# clear dot1x timeout supplicant
success: change accepted.
```

See Also

1 **set dot1x timeout supplicant** on page 524

1 **show dot1x** on page 526

clear dot1x tx-period

Resets to the default setting the number of seconds that must elapse before the UNIVERGE WL Controller retransmits an EAP over LAN (EAPoL) packet.

Syntax **clear dot1x tx-period**

Defaults The default is 5 seconds.

Access Enabled.

Examples Type the following command to reset the EAPoL retransmission time:

```
PROMPT# clear dot1x tx-period
success: change accepted.
```

See Also

1 **set dot1x tx-period** on page 524

1 **show dot1x** on page 526

set dot1x bonded-period

Changes the Bonded Auth™ (bonded authentication) period. The *Bonded Auth period* is the number of seconds UNIVERGE WL Control System allows a Bonded Auth user to reauthenticate.

Syntax **set dot1x bonded-period** *seconds*

seconds Number of seconds UNIVERGE WL Control System retains session information for an authenticated machine while waiting for a client to (re)authenticate on the same machine. You can change the bonded authentication period to a value from 1 to 300 seconds.

Defaults The default bonded period is 0 seconds, which disables the feature.

Access Enabled.

Usage Normally, the Bonded Auth period needs to be set only if the network has Bonded Auth clients that use dynamic WEP, or use WEP-40 or WEP-104 encryption with WPA or RSN. These clients can be affected by the 802.1X reauthentication parameter or the RADIUS Session-Timeout parameter.

UNIVERGE WL Control System recommends that you try 60 seconds, and change the period to a longer value only if clients are unable to authenticate within 60 seconds.

The bonded authentication period applies only to 802.1X authentication rules that contain the **bonded** option.

Examples To set the bonded authentication period to 60 seconds, type the following command:

```
PROMPT# set dot1x bonded-period 60
success: change accepted.
```

See Also

1 **clear dot1x bonded-period** on page 514

1 **show dot1x** on page 526

set dot1x key-tx

Enables or disables the transmission of encryption key information to the supplicant (client) in EAP over LAN (EAPoL) key messages, after authentication is successful.

Syntax **set dot1x key-tx {enable | disable}**

enable	Enables transmission of encryption key information to clients.
---------------	--

disable	Disables transmission of encryption key information to clients.
----------------	---

Defaults Key transmission is enabled by default.

Access Enabled.

set dot1x max-req

Chapter 17

Examples Type the following command to enable key transmission:

```
PROMPT# set dot1x key-tx enable
success: dot1x key transmission enabled.
```

See Also **show dot1x** on page 526

set dot1x max-req

Sets the maximum number of times the UNIVERGE WL Controller retransmits an EAP request to a supplicant (client) before ending the authentication session.

Syntax **set dot1x max-req** *number-of-retransmissions*

number-of-retransmissions Specify a value between 0 and 10.

Defaults The default number of EAP retransmissions is 2.

Access Enabled.

Usage To support SSIDs that have both 802.1X and static WEP clients, UNIVERGE WL Control System sends a maximum of two ID requests, even if this parameter is set to a higher value. Setting the parameter to a higher value does affect all other types of EAP messages.

Examples Type the following command to set the maximum number of EAP request retransmissions to three attempts:

```
PROMPT# set dot1x max-req 3
success: dot1x max request set to 3.
```

See Also

1 **clear dot1x max-req** on page 515

1 **show dot1x** on page 526

set dot1x quiet-period

Sets the number of seconds a UNIVERGE WL Controller remains quiet and does not respond to a supplicant after a failed authentication.

Syntax **set dot1x quiet-period** *seconds*

seconds Specify a value between 0 and 65,535.

Defaults The default is 60 seconds.

Access Enabled.

Examples Type the following command to set the quiet period to 90 seconds:

```
PROMPT# set dot1x quiet-period 90
success: dot1x quiet period set to 90.
```

See Also

- 1 **clear dot1x quiet-period** on page 515
- 1 **show dot1x** on page 526

set dot1x reauth

Determines whether the UNIVERGE WL Controller allows the reauthentication of supplicants (clients).

Syntax **set dot1x reauth** {**enable** | **disable**}

enable Permits reauthentication.

disable Denies reauthentication.

Defaults Reauthentication is enabled by default.

Access Enabled.

Examples Type the following command to enable reauthentication of supplicants (clients):

```
PROMPT# set dot1x reauth enable
success: dot1x reauthentication enabled.
```

See Also

- 1 **set dot1x reauth-max** on page 522
- 1 **set dot1x reauth-period** on page 522

- 1 **show dot1x** on page 526

set dot1x reauth-max

Sets the number of reauthentication attempts that the UNIVERGE WL Controller makes before the supplicant (client) becomes unauthorized.

Syntax **set dot1x reauth-max** *number-of-attempts*

number-of-attempts Specify a value between 1 and 10.

Defaults The default number of reauthentication attempts is 2.

Access Enabled.

Examples Type the following command to set the number of authentication attempts to 8:

```
PROMPT# set dot1x reauth-max 8
success: dot1x max reauth set to 8.
```

See Also

- 1 **clear dot1x reauth-max** on page 516
- 1 **show dot1x** on page 526

set dot1x reauth-period

Sets the number of seconds that must elapse before the UNIVERGE WL Controller attempts reauthentication.

Syntax **set dot1x reauth-period** *seconds*

seconds Specify a value between 60 (1 minute) and 1,641,600 (19 days).

Defaults The default is 3600 seconds (1 hour).

Access Enabled.

Usage You also can use the RADIUS session-timeout attribute to set the reauthentication timeout for a specific client. In this case, UNIVERGE WL Control System uses the timeout that has the lower value. If the session-timeout is set to fewer seconds than the global reauthentication timeout, UNIVERGE WL Control System uses the session-timeout for the client. However, if the global reauthentication timeout is shorter than the session-timeout, UNIVERGE WL Control System uses the global timeout instead.

Examples Type the following command to set the number of seconds to 100 before reauthentication is attempted:

```
PROMPT# set dot1x reauth-period 100
success: dot1x auth-server timeout set to 100.
```

See Also

1 **clear dot1x reauth-period** on page 516

1 **show dot1x** on page 526

set dot1x timeout auth-server

Sets the number of seconds that must elapse before the UNIVERGE WL Controller times out a request to a RADIUS authentication server.

Syntax **set dot1x timeout auth-server** *seconds*

seconds Specify a value between 1 and 65,535.

Defaults The default is 30 seconds.

Access Enabled.

Examples Type the following command to set the authentication server timeout to 60 seconds:

```
PROMPT# set dot1x timeout auth-server 60
success: dot1x auth-server timeout set to 60.
```

See Also

1 **clear dot1x timeout auth-server** on page 517

1 **show dot1x** on page 526

set dot1x timeout supplicant

Sets the number of seconds that must elapse before the UNIVERGE WL Controller times out an authentication session with a supplicant (client).

Syntax **set dot1x timeout supplicant** *seconds*

seconds Specify a value between 1 and 65,535.

Defaults The default is 30 seconds.

Access Enabled.

Examples Type the following command to set the number of seconds for authentication session timeout to 300:

```
PROMPT# set dot1x timeout supplicant 300
success: dot1x supplicant timeout set to 300.
```

See Also

- 1 **clear dot1x timeout auth-server** on page 517
- 1 **show dot1x** on page 526

set dot1x tx-period

Sets the number of seconds that must elapse before the UNIVERGE WL Controller retransmits an EAPoL packet.

Syntax **set dot1x tx-period** *seconds*

seconds Specify a value between 1 and 65,535.

Defaults The default is 5 seconds.

Access Enabled.

Examples Type the following command to set the number of seconds before the UNIVERGE WL Controller retransmits an EAPoL packet to 300:

```
PROMPT# set dot1x tx-period 300
```

success: dot1x tx-period set to 300.

See Also

- 1 **clear dot1x tx-period** on page 518
- 1 **show dot1x** on page 526

set dot1x wep-rekey

Enables or disables Wired Equivalency Privacy (WEP) rekeying for broadcast and multicast encryption keys.

Syntax **set dot1X wep-rekey {enable | disable}**

enable Causes the broadcast and multicast keys for WEP to be rotated at an interval set by the **set dot1x wep-rekey-period** for each radio, associated VLAN, and encryption type. The UNIVERGE WL Controller generates the new broadcast and multicast keys and pushes the keys to the clients via EAPoL key messages.

disable WEP broadcast and multicast keys are never rotated.

Defaults WEP key rotation is enabled, by default.

Access Enabled.

Usage Reauthentication is *not* required for WEP key rotation to take place. Broadcast and multicast keys are always rotated at the same time, so all members of a given radio, VLAN, or encryption type receive the new keys at the same time.

Examples Type the following command to disable WEP key rotation:

```
PROMPT# set dot1x wep-rekey disable
success: wep rekeying disabled
```

See Also

- 1 **set dot1x wep-rekey-period** on page 526
- 1 **show dot1x** on page 526

set dot1x wep-rekey-period

Sets the interval for rotating the WEP broadcast and multicast keys.

Syntax **set dot1x wep-rekey-period** *seconds*

seconds Specify a value between 30 and 1,641,600 (19 days).

Defaults The default is 1800 seconds (30 minutes).

Access Enabled.

Examples Type the following command to set the WEP-rekey period to 300 seconds:

```
PROMPT# set dot1x wep-rekey-period 300
success: dot1x wep-rekey-period set to 300
```

See Also

1 **set dot1x wep-rekey** on page 525

1 **show dot1x** on page 526

show dot1x

Displays 802.1X client information for statistics and configuration settings.

Syntax **show dot1x** {**clients** | **stats** | **config**}

clients Displays information about active 802.1X clients, including client name, MAC address, and state.

stats Displays global 802.1X statistics associated with connecting and authenticating.

config Displays a summary of the current configuration.

Defaults None.

Access Enabled.

Examples Type the following command to display the 802.1X clients:

PROMPT# show dot1x clients

MAC Address	State	Vlan	Identity
00:60:b9:48:01:1f	Connecting	(unknown)	
00:60:b9:07:6d:7c	Authenticated	vlan-it	EXAMPLE\jose
00:60:b9:7e:94:83	Authenticated	vlan-eng	EXAMPLE\singh
00:60:b9:86:bd:38	Authenticated	vlan-eng	bard@xmple.com
00:60:b9:7e:97:b4	Authenticated	vlan-eng	EXAMPLE\havel
00:60:b9:7e:98:1a	Authenticated	vlan-eng	EXAMPLE\nash
00:60:b9:a9:dc:4e	Authenticated	vlan-pm	xalik@xmple.com
00:60:b9:7e:96:e3	Authenticated	vlan-eng	EXAMPLE\mishan
00:60:b9:6f:44:77	Authenticated	vlan-eng	EXAMPLE\ethan
00:60:b9:7e:94:89	Authenticated	vlan-eng	EXAMPLE\fmarshall
00:60:b9:00:5c:02	Authenticated	vlan-eng	EXAMPLE\bmccarthy
00:60:b9:6a:de:f2	Authenticated	vlan-pm	neailey@xmple.com
00:60:b9:5e:5b:76	Authenticated	vlan-pm	EXAMPLE\tamara
00:60:b9:80:b6:e1	Authenticated	vlan-cs	dmc@xmple.com
00:60:b9:16:8d:69	Authenticated	vlan-wep	MAC authenticated
00:60:b9:64:8e:1b	Authenticated	vlan-eng	EXAMPLE\wong

Type the following command to display the 802.1X configuration:

PROMPT# show dot1x config

802.1X user policy

'host/bob-laptop.mycorp.com' on ssid 'mycorp' doing PASSTHRU
'bob.mycorp.com' on ssid 'mycorp' doing PASSTHRU (bonded)

802.1X parameter	setting
supplicant timeout	30
auth-server timeout	30
quiet period	5
transmit period	5
reauthentication period	3600
maximum requests	2
key transmission	enabled
reauthentication	enabled
authentication control	enabled
WEP rekey period	1800
WEP rekey	enabled
Bonded period	60

Type the following command to display 802.1X statistics:

PROMPT# show dot1x stats

802.1X statistic	value
-----	-----

show dot1x

Chapter 17

```
Enters Connecting:          709
Logoffs While Connecting:   112
Enters Authenticating:      467
Success While Authenticating: 0
Timeouts While Authenticating: 52
Failures While Authenticating: 0
Reauths While Authenticating: 0
Starts While Authenticating: 31
Logoffs While Authenticating: 0
Starts While Authenticated: 85
Logoffs While Authenticated: 1
Bad Packets Received:       0
```

Table 61 explains the counters in the **show dot1x stats** output.

Table 61. show dot1x stats Output

Field	Description
Enters Connecting	Number of times that the UNIVERGE WL Controller state transitions to the CONNECTING state from any other state.
Logoffs While Connecting	Number of times that the UNIVERGE WL Controller state transitions from CONNECTING to DISCONNECTED as a result of receiving an EAPoL-Logoff message.
Enters Authenticating	Number of times that the state wildcard transitions.
Success While Authenticating	Number of times the UNIVERGE WL Controller state transitions from AUTHENTICATING from AUTHENTICATED, as a result of an EAP-Response/Identity message being received from the supplicant (client).
Timeouts While Authenticating	Number of times that the UNIVERGE WL Controller state wildcard transitions from AUTHENTICATING to ABORTING.
Failures While Authenticating	Number of times that the UNIVERGE WL Controller state wildcard transitions from AUTHENTICATION to HELD.

Table 61. show dot1x stats Output

Field	Description
Reauths While Authenticating	Number of times that the UNIVERGE WL Controller state wildcard transitions from AUTHENTICATING to ABORTING, as a result of a reauthentication request (reAuthenticate = TRUE).
Starts While Authenticating	Number of times that the UNIVERGE WL Controller state wildcard transitions from AUTHENTICATING to ABORTING, as a result of an EAPoL-Start message being received from the Supplicant (client).
Logoffs While Authenticating	Number of times that the UNIVERGE WL Controller state wildcard transitions from AUTHENTICATING to ABORTING, as a result of an EAPoL-logoff message being received from the Supplicant (client).
Bad Packets Received	Number of EAPoL packets received that have an invalid version or type.

show dot1x

Chapter 17

Session Management Commands

Use session management commands to display and clear administrative and network user sessions. This chapter presents session management commands alphabetically. Use the following table to locate commands in this chapter based on their use.

Administrative Sessions	show sessions on page 534
	clear sessions on page 531
Network Sessions	show sessions network on page 536
	clear sessions network on page 532

clear sessions

Clears all administrative sessions, or clears administrative console or Telnet sessions.

Syntax **clear sessions** { **admin** | **console** | **telnet** [**client** *session-id*] | **mesh-ap** [**session-id** *session-id*] }

admin	Clears sessions for all users with administrative access to the UNIVERGE WL Controller through a Telnet or SSH connection or a console plugged into the UNIVERGE WL Controller.
console	Clears sessions for all users with administrative access to the UNIVERGE WL Controller through a console plugged into the UNIVERGE WL Controller.

clear sessions network

Chapter 18

telnet	Clears sessions for all users with administrative access to the UNIVERGE WL Controller through a Telnet connection.
telnet client [<i>session-id</i>]	Clears all Telnet client sessions from the CLI to remote devices, or clears an individual session identified by session ID.
mesh-ap [<i>session-id</i>]	Note: This parameter is not supported.

Defaults None.

Access Enabled.

Examples To clear all administrator sessions type the following command:

```
PROPMT# clear sessions admin
This will terminate manager sessions, do you wish to continue? (y|n) [n]y
```

To clear all administrative sessions through the console, type the following command:

```
PROPMT# clear sessions console
This will terminate manager sessions, do you wish to continue? (y|n) [n]y
```

To clear all administrative Telnet sessions, type the following command:

```
PROPMT# clear sessions telnet
This will terminate manager sessions, do you wish to continue? (y|n) [n]y
```

To clear Telnet client session 0, type the following command:

```
PROPMT# clear sessions telnet client 0
```

See Also **show sessions** on page 534

clear sessions network

Clears all network sessions for a specified username or set of usernames, MAC address or set of MAC addresses, virtual LAN (VLAN) or set of VLANs, or session ID.

Syntax **clear sessions network** {**user** *user-glob* | **mac-addr** *mac-addr-glob* | **vlan** *vlan-glob* | **session-id** *local-session-id*}

user <i>user-glob</i>	<p>Clears all network sessions for a single user or set of users.</p> <p>Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an <i>at</i> sign (@) or a period (.). (For details, see “User Globs” on page 9.)</p>
mac-addr <i>mac-addr-glob</i>	<p>Clears all network sessions for a MAC address. Specify a MAC address in hexadecimal numbers separated by colons (:), or use the wildcard character (*) to specify a set of MAC addresses. (For details, see “MAC Address Globs” on page 10.)</p>
vlan <i>vlan-glob</i>	<p>Clears all network sessions on a single VLAN or a set of VLANs.</p> <p>Specify a VLAN name, use the double-asterisk wildcard character (**) to specify all VLAN names, or use the single-asterisk wildcard character (*) to specify a set of VLAN names up to or following the first delimiter character, either an <i>at</i> sign (@) or a period (.). (For details, see “VLAN Globs” on page 10.)</p>
session-id <i>local-session-id</i>	<p>Clears the specified 802.1X network session. To find local session IDs, use the show sessions command.</p>

Defaults None.

Access Enabled.

Usage The **clear sessions network** command clears network sessions by deauthenticating and, for wireless clients, disassociating them.

Examples To clear all sessions for MAC address 00:01:02:03:04:05, type the following command:

```
PROPMT# clear sessions network mac-addr 00:01:02:03:04:05
```

To clear session 9, type the following command:

```
Controller# clear sessions network session-id 9
SM Apr 11 19:53:38 DEBUG SM-STATE: localid 9, mac 00:60:25:09:39:5d,
flags 0000012fh, to change state to KILLING
Localid 9, globalid SESSION-9-893249336 moved from ACTIVE to KILLING
(client=00:60:25:09:39:5d)
```

To clear the session of user *Natasha*, type the following command:

```
Controller# clear sessions network user Natasha
```

To clear the sessions of users whose name begins with the characters *Jo*, type the following command:

```
Controller# clear sessions network user Jo*
```

To clear the sessions of all users on VLAN *red*, type the following command:

```
Controller# clear sessions network vlan red
```

See Also

- 1 **show sessions** on page 534
- 1 **show sessions network** on page 536

show sessions

Displays session information and statistics for all users with administrative access to the UNIVERGE WL Controller, or for administrative users with either console or Telnet access.

Syntax **show sessions** { **admin** | **console** | **telnet** [**client**] }

admin	Displays sessions for all users with administrative access to the UNIVERGE WL Controller through a Telnet or SSH connection or a console plugged into the UNIVERGE WL Controller.
console	Displays sessions for all users with administrative access to the UNIVERGE WL Controller through a console plugged into the UNIVERGE WL Controller.

- telnet** Displays sessions for all users with administrative access to the UNIVERGE WL Controller through a Telnet connection.
- telnet client** Displays Telnet sessions from the CLI to remote devices.

Defaults None.

Access All, except for **show sessions telnet client**, which has enabled access.

Examples To view information about sessions of administrative users, type the following command:

```
PROMPT> show sessions admin
Tty      Username      Time (s)   Type
-----
tty0          tech          3644      Telnet(172.16.221.2)
tty2          sshadmin       6          Telnet(172.16.221.3)
tty3          sshadmin       381        SSH(172.16.221.5)

3 admin sessions
```

To view information about console users' sessions, type the following command:

```
PROMPT> show sessions console
Tty      Username      Time (s)
-----
console          8573

1 console session
```

To view information about Telnet users sessions, type the following command:

```
PROMPT> show sessions telnet
Tty      Username      Time (s)
-----
tty2          sea          7395 telnet(172.16.221.3)
```

To view information about Telnet client sessions, type the following command:

```
PROMPT# show sessions telnet client
Session  Server Address  Server Port  Client Port
-----
0         192.168.1.81    23           48000
1         10.10.1.22      23           48001
```

Table 62 describes the fields of the **show sessions admin**, **show sessions console**, and **show sessions telnet** displays.

Table 63 describes the fields of the **show sessions telnet client** display.

Table 62. show sessions admin, show sessions console, and show sessions telnet Output

Field	Description
Tty	The Telnet terminal number, or <i>console</i> for administrative users connected through the console port.
Username	Up to 30 characters of the name of an authenticated user.
Time (s)	Number of seconds the session has been active.
Type	Type of administrative session: <ul style="list-style-type: none">• Console• SSH• Telnet

Table 63. show sessions telnet client Output

Field	Description
Session	Session number assigned by UNIVERGE WL Control System when the client session is established.
Server Address	IP address of the remote device.
Server Port	TCP port number of the remote device's TCP server.
Client Port	TCP port number UNIVERGE WL Control System is using for the client side of the session.

See Also `clear sessions` on page 531

show sessions network

Displays summary or verbose information about all network sessions, or network sessions for a specified username or set of usernames, MAC address or set of MAC addresses, VLAN or set of VLANs, or session ID.

Syntax **show sessions network** [**user** *user-glob* | **mac-addr** *mac-addr-glob* | **ssid** *ssid-name* | **vlan** *vlan-glob* | **session-id** *session-id*] [**verbose**]

user <i>user-glob</i>	Displays all network sessions for a single user or set of users. Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an <i>at</i> sign (@) or a period (.). (For details, see “User Globs” on page 9.)
mac-addr <i>mac-addr-glob</i>	Displays all network sessions for a MAC address. Specify a MAC address in hexadecimal numbers separated by colons (:). Or use the wildcard character (*) to specify a set of MAC addresses. (For details, see “MAC Address Globs” on page 10.)
ssid <i>ssid-name</i>	Displays all network sessions for an SSID.
vlan <i>vlan-glob</i>	Displays all network sessions on a single VLAN or a set of VLANs. Specify a VLAN name, use the double-asterisk wildcard character (**) to specify all VLAN names, or use the single-asterisk wildcard character (*) to specify a set of VLAN names up to or following the first delimiter character, either an <i>at</i> sign (@) or a period (.). (For details, see “VLAN Globs” on page 10.)
session-id <i>local-session-id</i>	Displays the specified network session. To find local session IDs, use the show sessions command. The verbose option is not available with this form of the show sessions network command.
verbose	Provides detailed output for all network sessions or ones displayed by username, MAC address, or VLAN name.

Defaults None.

Access All.

show sessions network

Chapter 18

Usage UNIVERGE WL Control System displays information about network sessions in three types of displays. See the following tables for field descriptions.

Summary display See Table 64 on page 540.

Verbose display See Table 65 on page 541.

show sessions network session-id display See Table 66 on page 543.

Authorization attribute values can be changed during authorization. If the values are changed, **show sessions** output shows the values that are actually in effect following any changes.

Examples To display summary information for all network sessions, type **show sessions network**. For example:

```
PROMPT> show sessions network
User      Sess  IP or MAC      VLAN      Port/
Name      ID    Address        Name      Radio
-----
EXAMPLE\Natasha      4*  10.10.40.17    vlan-eng   ap 3/1
host/laptop11.exmpl.com 6*  10.10.40.16    vlan-eng   ap 3/2
nin@exmpl.com      539* 10.10.40.17    vlan-eng   ap 1/1
EXAMPLE\hosni      302* 10.10.40.10    vlan-eng   ap 3/1
                        563  00:0b:be:15:46:56 (none)     1/2
jose@exmpl.com      380* 10.30.40.8      vlan-eng   ap 1/1
00:30:65:16:8d:69    443* 10.10.40.19    vlan-wep   ap 3/1
EXAMPLE\Geetha      459* 10.10.40.18    vlan-eng   ap 3/2
8 sessions total
```

The following command displays summary information about the sessions for MAC address 00:60:b9:7e:98:1a:

```
PROMPT> show sessions network mac-addr 00:60:b9:7e:98:1a
User      Sess  IP or MAC      VLAN      Port/
Name      ID    Address        Name      Radio
-----
EXAMPLE\Havel      13*  10.10.10.40    vlan-eng   ap 1/2
```

The following command displays summary information about all the sessions of users whose names begin with *E*:

```
PROMPT> show sessions network user E*
User      Sess  IP or MAC      VLAN      Port/
Name      ID    Address        Name      Radio
-----
EXAMPLE\Singh      12*  10.10.10.30    vlan-eng   ap 3/2
```

```
EXAMPLE\Havel          13* 10.10.10.40    vlan-eng    ap 1/2
2 sessions match criteria (of 3 total)
```

(Table 64 on page 540 describes the summary displays of **show sessions network** commands.)

The following command displays verbose output about the sessions of all current network users:

```
PROMPT> show sessions network verbose
User          Sess IP or MAC      VLAN          Port/
Name          ID   Address       Name          Radio
-----
SHUTTLE2\exmpl      3* 10.8.255.8   default       7/1
Client MAC: 00:60:b9:22:b1:fb GID: SESS-3-00040c-287058-657673d4
State: ACTIVE      (prev AUTHORIZED)
now on: switch 172.16.0.1, ap 1, AP/radio G8TZUB0028/1, as of 00:00:22 ago
      from: switch 172.16.0.1, ap 3, AP/radio G8TZUB0038/1, as of 00:01:07 ago
      from: switch 172.16.0.1, ap 2, AP/radio G8TZUB0428/1, as of 00:01:53 ago

Host name: shuttle2_laptop
Vlan-Name=default (service-profile)
Service-Type=2 (service-profile)
End-Date=52/06/07-08:57 (AAA)
Start-Date=05/04/11-10:00 (AAA)

1 sessions total
```

(Table 65 on page 541 describes the additional fields of the **verbose** output of **show sessions network** commands.)

The following command displays information about network session 88:

```
PROMPT# show sessions network session-id 88
Local Id:      88
Global Id:     SESS-88-00040f-876766-623fd6
State:         ACTIVE
SSID:          Rack-39-PM
Port/Radio:    ap 1/1
MAC Address:   00:60:b9:11:71:6d
User Name:     last-resort-Rack-39-PM
IP Address:    10.2.39.217
Vlan Name:     default
Tag:           1
Session Start: Wed Apr 12 21:19:27 2006 GMT
Last Auth Time: Wed Apr 12 21:19:26 2006 GMT
Last Activity: Wed Apr 12 21:19:49 2006 GMT ( <15s ago)
Session Timeout: 0
Idle Time-To-Live: 175
Login Type:    LAST-RESORT
```

show sessions network

Chapter 18

```
EAP Method:      NONE, using server 172.16.0.1
Session statistics as updated from AP:
Unicast packets in: 31
Unicast bytes in: 3418
Unicast packets out: 18
Unicast bytes out: 2627
Multicast packets in: 0
Multicast bytes in: 0
Number of packets with encryption errors: 0
Number of bytes with encryption errors: 0
Last packet data rate: 48
Last packet signal strength: -60 dBm
Last packet data S/N ratio: 35
Protocol: voice-ext
Requested bandwidth (bytes/s): 92800
Session CAC: disabled
```

For descriptions of the fields of **show sessions network session-id** output, see Table 66 on page 543.

Table 64. show sessions network (summary) Output

Field	Description
User Name	Up to 30 characters of the name of the authenticated user of this session. Note: For a MAC-authenticated session, this value is the client device's MAC address.
Sess ID	Locally unique number that identifies this session. An asterisk (*) next to a session ID indicates that the session is fully active.
IP or MAC Address	IP address of the session user, or the user's MAC address if the user has not yet received an IP address.
VLAN Name	Name of the VLAN associated with the session.
Port/Radio	Ap number and radio through which the user is accessing this session.

Table 65. Additional show sessions network verbose Output

Field	Description
Client MAC	MAC address of the session user.
GID	Global session ID, a unique session number within a Mobility Domain.
State	<p>Status of the session:</p> <ul style="list-style-type: none"> • AUTH, ASSOC REQ—Client is being associated by the 802.1X protocol. • AUTH AND ASSOC—Client is being associated by the 802.1X protocol, and the user is being authenticated. • AUTHORIZING—User has been authenticated (for example, by the 802.1X protocol and an AAA method), and is entering AAA authorization. • AUTHORIZED—User has been authorized by an AAA method. • ACTIVE—User's AAA attributes have been applied, and the user is active on the network. • DEASSOCIATED—One of the following: <ul style="list-style-type: none"> • Wireless client has sent the UNIVERGE WL Controller a disassociate message. • User associated with one of the current UNIVERGE WL Controller's AP has appeared at another UNIVERGE WL Controller in the Mobility Domain. • ROAMING AWAY—The UNIVERGE WL Controller has been sent a request to transfer the user, who is roaming, to another UNIVERGE WL Controller. • STATUS UPDATED—UNIVERGE WL Controller is receiving a final update from an AP about the user, who has roamed away. • WEB_AUTHING—User is being authenticated by WebAAA. • KILLING—User's session is being cleared, because of 802.1X authentication failure, entry of a clear command, or some other event.

Table 65. Additional show sessions network verbose Output

Field	Description
now on	Shows the following information about the UNIVERGE WL Access Points and radio the session is currently on: <ul style="list-style-type: none">• IP address and port number of the UNIVERGE WL Controller managing the UNIVERGE WL Access Points• Serial number and radio number of the UNIVERGE WL Access Points• Amount of time the session has been on this UNIVERGE WL Access Points
from	Shows information about the UNIVERGE WL Access Points from which the session has roamed. (See the descriptions above for the <i>now on</i> field.)
Host name	Host name of the user's networking device.

Table 65. Additional show sessions network verbose Output

Field	Description
Vlan-Name (and other attributes if set)	<p>Authorization attributes for the user and how they were assigned (the sources of the attribute values).</p> <p>For Vlan-Name, the source of the attribute value can be one of the following:</p> <ul style="list-style-type: none"> • AAA—VLAN is from RADIUS or the local database. • initial-assignment—For a client that has roamed from one UNIVERGE WL Controller to another, VLAN is the one assigned to the user on the UNIVERGE WL Controller where the user first accessed the network. (This is the UNIVERGE WL Controller where the client's global session in the Mobility Domain started.) <p>This authorization source (<i>initial-assignment</i>) is displayed only if the following conditions are true:</p> <ul style="list-style-type: none"> • The client roamed from another UNIVERGE WL Controller. • The service profile for the SSID the user is on is configured to keep the client's initial VLAN assignment. (This means the keep-initial-vlan option is enabled on the service profile.) • The VLAN is not configured for the user on the roamed-to switch by the local database. • A Location Policy on the roamed-to UNIVERGE WL Controller does not set the VLAN. • location policy—Attribute value was assigned by a Location Policy. • service-profile—Attribute value is configured on the SSID, and was not overridden by other attribute sources (such as AAA or location policy). • Web Portal—Session is for a Web Portal client.

Table 66. show sessions network session-id Output

Field	Description
Local Id	Identifier for the session on this particular UNIVERGE WL Controller. (This is the session ID you specify when entering the show sessions network session-id command.)
Global Id	Unique session identifier within the Mobility Domain.

Table 66. show sessions network session-id Output

Field	Description
State	<p>Status of the session:</p> <ul style="list-style-type: none"> • AUTH, ASSOC REQ—Client is being associated by the 802.1X protocol. • AUTH AND ASSOC—Client is being associated by the 802.1X protocol, and the user is being authenticated. • AUTHORIZING—User has been authenticated (for example, by the 802.1X protocol and an AAA method), and is entering AAA authorization. • AUTHORIZED—User has been authorized by an AAA method. • ACTIVE—User's AAA attributes have been applied, and the user is active on the network. • DEASSOCIATED—One of the following: <ul style="list-style-type: none"> • Wireless client has sent the UNIVERGE WL Controller a disassociate message. • User associated with one of the current UNIVERGE WL Controllers AP has appeared at another UNIVERGE WL Controller in the Mobility Domain. • ROAMING AWAY—The UNIVERGE WL Controller has been sent a request to transfer the user, who is roaming, to another UNIVERGE WL Controller. • STATUS UPDATED—UNIVERGE WL Controller is receiving a final update from an AP about the user, who has roamed away. • WEB_AUTHING—User is being authenticated by WebAAA. • KILLING—User's session is being cleared, because of 802.1X authentication failure, entry of a clear command, or some other event.
SSID	Name of the SSID the user is on.
Port/Radio	AP number and radio through which the user is accessing this session.
MAC address	MAC address of the session user.
User Name	Name of the authenticated user of this session
IP Address	IP address of the session user.
Vlan Name	Name of the VLAN associated with the session.

Table 66. show sessions network session-id Output

Field	Description
Tag	System-wide supported VLAN tag type.
Session Start	Indicates when the session started.
Last Auth Time	Indicates when the most recent authentication of the session occurred.
Last Activity	Indicates when the last activity (transmission) occurred on the session.
Session Timeout	Assigned session timeout in seconds.
Idle Time-To-Live	Number of seconds the session can remain idle before UNIVERGE WL Control System changes the session state to Disassociated.
Login Type	Authentication type used to log onto the network: <ul style="list-style-type: none"> • DOT1X • MAC • LAST-RESORT • WEB-PORTAL
EAP Method	Extensible Authentication Protocol (EAP) type used to authenticate the session user, and the IP address of the authentication server.
Session statistics as updated from AP	Time the session statistics were last updated from the AP, in seconds since a fixed standard date and time.
Unicast packets in	Total number of unicast packets received from the user by the UNIVERGE WL Controller (64-bit counter).
Unicast bytes in	Total number of unicast bytes received from the user by the UNIVERGE WL Controller (64-bit counter).
Unicast packets out	Total number of unicast packets sent by the UNIVERGE WL Controller to the user (64-bit counter).
Unicast bytes out	Total number of unicast bytes sent by the UNIVERGE WL Controller to the user (64-bit counter).
Multicast packets in	Total number of multicast packets received from the user by the UNIVERGE WL Controller (64-bit counter).
Multicast bytes in	Total number of multicast bytes received from the user by the UNIVERGE WL Controller (64-bit counter).

Table 66. show sessions network session-id Output

Field	Description
Number of packets with encryption errors	Total number of decryption failures.
Number of bytes with encryption errors	Total number of bytes with decryption errors.
Last packet data rate	Data transmit rate, in megabits per second (Mbps), of the last packet received by the AP.
Last packet signal strength	Signal strength, in decibels referred to 1 milliwatt (dBm), of the last packet received by the AP.
Last packet data S/N ratio	Signal-to-noise ratio of the last packet received by the AP.
Protocol	Wireless protocol used: <ul style="list-style-type: none">• 802.11 (for WMM and SVP QoS modes)• voice-ext (for Voice-Extension QoS mode)
Requested Bandwidth	Number of bytes reserved on the radio for this session. (This value applies only when the QoS mode and CAC mode are both Voice-Extension.)
Session CAC	State of session-based Call Admission Control (CAC) on the SSID's service profile.

See Also `clear sessions network` on page 532

RF Detection Commands

UNIVERGE WL Control System automatically performs RF detection scans on enabled and disabled radios to detect rogue access points. A rogue access point is a BSSID (MAC address associated with an SSID) that does not belong to a UNIVERGE WL Control System device and is not a member of the ignore list configured on the seed UNIVERGE WL Controller of the Mobility Domain.

UNIVERGE WL Control System can issue countermeasures against rogue devices to prevent clients from being able to use them.

You can configure RF detection parameters on individual UNIVERGE WL Controller.

This chapter presents RF detection commands alphabetically. Use the following table to locate the commands in this chapter based on their use.

Rogue Information	show rfdetect clients on page 560
	show rfdetect mobility-domain on page 568
	show rfdetect data on page 566
	show rfdetect visible on page 574
	show rfdetect counters on page 564
Countermeasures	show rfdetect countermeasures on page 563
Permitted Vendor List	set rfdetect vendor-list on page 558
	show rfdetect vendor-list on page 573
	clear rfdetect vendor-list on page 550
Permitted SSID List	set rfdetect ssid-list on page 557
	show rfdetect ssid-list on page 573
	clear rfdetect ssid-list on page 550

Client Black List	set rfdetect black-list on page 553 show rfdetect black-list on page 559 clear rfdetect black-list on page 549
Attack List	set rfdetect attack-list on page 552 show rfdetect attack-list on page 559 clear rfdetect attack-list on page 548
Ignore List	set rfdetect ignore on page 554 show rfdetect ignore on page 568 clear rfdetect ignore on page 549
UNIVERGE WL Access Points Signatures	set rfdetect signature on page 556
Log Messages	set rfdetect log on page 555
UNIVERGE WL Controller-to-Client RF Link	rfping on page 551

clear rfdetect attack-list

Removes a MAC address from the attack list.

Syntax **clear rfdetect attack-list** *mac-addr*

mac-addr MAC address you want to remove from the attack list.

Defaults None.

Access Enabled.

Examples The following command clears MAC address 11:22:33:44:55:66 from the attack list:

```
PROPMT# clear rfdetect attack-list 11:22:33:44:55:66
success: 11:22:33:44:55:66 is no longer in attacklist.
```

See Also

- 1 **set rfdetect attack-list** on page 552
- 1 **show rfdetect attack-list** on page 559

clear rfdetect black-list

Removes a MAC address from the client black list.

Syntax **clear rfdetect black-list** *mac-addr*

mac-addr MAC address you want to remove from the black list.

Defaults None.

Access Enabled.

Examples The following command removes MAC address 11:22:33:44:55:66 from the black list:

```
PROPMT# clear rfdetect black-list 11:22:33:44:55:66
success: 11:22:33:44:55:66 is no longer blacklisted.
```

See Also

- 1 **set rfdetect black-list** on page 553
- 1 **show rfdetect black-list** on page 559

clear rfdetect ignore

Removes a device from the ignore list for RF scans. UNIVERGE WL Control System does not generate log messages or traps for the devices in the ignore list.

Syntax **clear rfdetect ignore** *mac-addr*

mac-addr Basic service set identifier (BSSID), which is a MAC address, of the device to remove from the ignore list.

Defaults None.

clear rfdetect ssid-list

Chapter 19

Access Enabled.

Examples The following command removes BSSID *aa:bb:cc:11:22:33* from the ignore list for RF scans:

```
AP clear rfdetect ignore aa:bb:cc:11:22:33
success: aa:bb:cc:11:22:33 is no longer ignored.
```

See Also

- 1 **set rfdetect ignore** on page 554
- 1 **show rfdetect ignore** on page 568

clear rfdetect ssid-list

Removes an SSID from the permitted SSID list.

Syntax **clear rfdetect ssid-list** *ssid-name*

ssid-name SSID name you want to remove from the permitted SSID list.

Defaults None.

Access Enabled.

Examples The following command clears SSID *mycorp* from the permitted SSID list:

```
PROPMT# clear rfdetect ssid-list mycorp
success: mycorp is no longer in ssid-list.
```

See Also

- 1 **set rfdetect ssid-list** on page 557
- 1 **show rfdetect ssid-list** on page 573

clear rfdetect vendor-list

Removes an entry from the permitted vendor list.

Syntax `clear rfdetect vendor-list {client mac-addr | all}`

client | ap Specifies whether the entry is for an AP brand or a client brand.

***mac-addr* | all** Organizationally Unique Identifier (OUI) to remove.

Defaults None.

Access Enabled.

Examples The following command removes client OUI aa:bb:cc:00:00:00 from the permitted vendor list:

```
PROPMT# clear rfdetect vendor-list client aa:bb:cc:00:00:00
success: aa:bb:cc:00:00:00 is no longer in client vendor-list.
```

See Also

- 1 **set rfdetect vendor-list** on page 558
- 1 **show rfdetect vendor-list** on page 573

rfping

Provides information about the RF link between the UNIVERGE WL Controller and the client based on sending test packets to the client.

Syntax `rfping {mac mac-addr | session-id session-id}`

mac-addr Tests the RF link between the UNIVERGE WL Controller and the client with the specified MAC address.

session-id Tests the RF link between the UNIVERGE WL Controller and the client with the specified local session ID.

Defaults None.

Access Enabled.

Usage Use this command to send test packets to a specified client. The output of the command indicates the number of test packets received and acknowledged by the client, as well as the client's signal strength and signal-to-noise ratio.

set rfdetect attack-list

Chapter 19

Examples The following command tests the RF link between the UNIVERGE WL Controller and the client with MAC address 00:60:b9:11:ad:13:

```
PROPMTH# rfping mac 00:60:b9:11:ad:13
RF-Link Test to 00:60:b9:11:ad:13 :
Session-Id: 2
Packets Sent   Packets Rcvd   RSSI      SNR      RTT (micro-secs)
-----
                20             20       -68      26       976
```

Table 67 describes the fields in this display.

Table 67. rfping Output

Field	Description
Packets Sent	The number of test packets sent from the UNIVERGE WL Controller to the client.
Packets Rcvd	The number of test packets acknowledged by the client.
RSSI	Received signal strength indication (RSSI)—the strength of the RF signal from the client, in decibels referred to 1 milliwatt (dBm).
SNR	Signal-to-noise ratio (SNR), in decibels (dB), of the data received from the client.
RTT (micro-secs)	The round-trip time, in microseconds, for the client response to the test packets.

See Also

- 1 **show rfdetect data** on page 566
- 1 **show rfdetect visible** on page 574

set rfdetect attack-list

Adds an entry to the attack list. The attack list specifies the MAC addresses of devices that UNIVERGE WL Control System should issue countermeasures against whenever the devices are detected on the network. The attack list can contain the MAC addresses of APs and clients.

Syntax `set rfdetect attack-list mac-addr`

mac-addr MAC address you want to attack.

Defaults The attack list is empty by default.

Access Enabled.

Usage The attack list applies only to the UNIVERGE WL Controller on which the list is configured. UNIVERGE WL Controllers do not share attack lists.

When on-demand countermeasures are enabled (with the **set radio-profile countermeasures configured** command) only those devices configured in the attack list are subject to countermeasures. In this case, devices found to be rogues by other means, such as policy violations or by determining that the device is providing connectivity to the wired network, are not attacked.

Examples The following command adds MAC address aa:bb:cc:44:55:66 to the attack list:

```
PROPMT# set rfdetect attack-list 11:22:33:44:55:66
success: MAC 11:22:33:44:55:66 is now in attacklist.
```

See Also

- 1 **clear rfdetect attack-list** on page 548
- 1 **show rfdetect attack-list** on page 559
- 1 **set radio-profile countermeasures** on page 307

set rfdetect black-list

Adds an entry to the client black list. The client black list specifies clients that are not allowed on the network. UNIVERGE WL Control System drops all packets from the clients on the black list.

Syntax `set rfdetect black-list mac-addr`

mac-addr MAC address you want to place on the black list.

set rfdetect ignore

Chapter 19

Defaults The client black list is empty by default.

Access Enabled.

Usage In addition to manually configured entries, the list can contain entries added by UNIVERGE WL Control System. UNIVERGE WL Control System can place a client in the black list due to an association, reassociation or disassociation flood from the client.

The client black list applies only to the UNIVERGE WL Controller on which the list is configured. UNIVERGE WL Controllers do not share client black lists.

Examples The following command adds client MAC address 11:22:33:44:55:66 to the black list:

```
PROPMT# set rfdetect black-list 11:22:33:44:55:66
success: MAC 11:22:33:44:55:66 is now blacklisted.
```

See Also

- 1 **set rfdetect black-list** on page 553
- 1 **show rfdetect black-list** on page 559

set rfdetect ignore

Configures a list of known devices to ignore during an RF scan. UNIVERGE WL Control System does not generate log messages or traps for the devices in the ignore list.

Syntax **set rfdetect ignore** *mac-addr*

mac-addr BSSID (MAC address) of the device to ignore.

Defaults UNIVERGE WL Control System reports all non-UNIVERGE WL Control System BSSIDs detected during an RF scan.

Access Enabled.

Usage Use this command to identify third-party APs and other devices you are already aware of and do not want UNIVERGE WL Control System to report following RF scans.

If you try to initiate countermeasures against a device on the ignore list, the ignore list takes precedence and UNIVERGE WL Control System does not issue the countermeasures. Countermeasures apply only to rogue devices.

If you add a device that UNIVERGE WL Control System has classified as a rogue to the permitted vendor list or permitted SSID list, but not to the ignore list, UNIVERGE WL Control System can still classify the device as a rogue. Adding an entry to the permitted vendor list or permitted SSID list merely indicates that the device is from an allowed manufacturer or is using an allowed SSID. However, to cause UNIVERGE WL Control System to stop classifying the device as a rogue, you must add the device's MAC address to the ignore list.

Examples The following command configures UNIVERGE WL Control System to ignore BSSID *aa:bb:cc:11:22:33* during RF scans:

```
Controller# set rfdetect ignore aa:bb:cc:11:22:33
success: MAC aa:bb:cc:11:22:33 is now ignored.
```

See Also

- 1 **clear rfdetect ignore** on page 549
- 1 **show rfdetect ignore** on page 568

set rfdetect log

Disables or reenables generation of log messages when rogues are detected or when they disappear.

Syntax `set rfdetect log {enable | disable}`

enable Enables logging of rogues.

disable Disables logging of rogues.

Defaults RF detection logging is enabled by default.

Access Enabled.

set rfdetect signature

Chapter 19

Usage The log messages for rogues are generated only on the seed and appear only in the seed's log message buffer. Use the **show log buffer** command to display the messages in the seed UNIVERGE WL Controllers log message buffer.

Examples The following command enables RF detection logging for the Mobility Domain managed by this seed UNIVERGE WL Controller:

```
Controller# set rfdetect log enable
success: rfdetect logging is enabled.
```

See Also **show log buffer** on page 630

set rfdetect signature

Enables UNIVERGE WL Access Points signatures. A UNIVERGE WL Access Point signature is a set of bits in a management frame sent by a UNIVERGE WL Access Point that identifies that UNIVERGE WL Access Points to UNIVERGE WL Control System. If someone attempts to spoof management packets from a UNIVERGE WL Access Points, UNIVERGE WL Control System can detect the spoof attempt.

Syntax **set rfdetect signature** {**enable** | **disable**}

enable Enables UNIVERGE WL Access Points signatures.

disable Disables UNIVERGE WL Access Points signatures.

Defaults UNIVERGE WL Access Points signatures are disabled by default.

Access Enabled.

Usage The command applies only to UNIVERGE WL Access Points managed by the UNIVERGE WL Controller on which you enter the command. To enable signatures on all UNIVERGE WL Access Points in a Mobility Domain, enter the command on each UNIVERGE WL Controller in the Mobility Domain.



Note. You must use the same UNIVERGE WL Access Points signature setting (enabled or disabled) on all UNIVERGE WL Controllers in a Mobility Domain.

Examples The following command enables UNIVERGE WL Access Points signatures on a UNIVERGE WL Controller:

```
Controller# set rfdetect signature enable
success: signature is now enabled.
```

set rfdetect ssid-list

Adds an SSID to the permitted SSID list. The permitted SSID list specifies the SSIDs that are allowed on the network. If UNIVERGE WL Control System detects packets for an SSID that is not on the list, the AP that sent the packets is classified as a rogue. UNIVERGE WL Control System issues countermeasures against the rogue if they are enabled.

Syntax `set rfdetect ssid-list ssid-name`

ssid-name SSID name you want to add to the permitted SSID list.

Defaults The permitted SSID list is empty by default and all SSIDs are allowed. However, after you add an entry to the list, UNIVERGE WL Control System allows traffic only for the SSIDs that are on the list.

Access Enabled.

Usage The permitted SSID list applies only to the UNIVERGE WL Controller on which the list is configured. UNIVERGE WL Controllers do not share permitted SSID lists.

If you add a device that UNIVERGE WL Control System has classified as a rogue to the permitted SSID list, but not to the ignore list, UNIVERGE WL Control System can still classify the device as a rogue. Adding an entry to the permitted SSID list merely indicates that the device is using an allowed SSID. However, to cause UNIVERGE WL Control System to stop classifying the device as a rogue, you must add the device's MAC address to the ignore list.

Examples The following command adds SSID *mycorp* to the list of permitted SSIDs:

```
PROPMT# set rfdetect ssid-list mycorp
success: ssid mycorp is now in ssid-list.
```

See Also

- 1 **clear rfdetect ssid-list** on page 550
- 1 **show rfdetect ssid-list** on page 573

set rfdetect vendor-list

Adds an entry to the permitted vendor list. The permitted vendor list specifies the third-party AP or client vendors that are allowed on the network. UNIVERGE WL Control System does not list a device as a rogue or interfering device if the device's OUI is in the permitted vendor list.

Syntax **set rfdetect vendor-list** { **client** | **ap** } *mac-addr*

client | **ap** Specifies whether the entry is for an AP brand or a client brand.

mac-addr | **all** Organizationally Unique Identifier (OUI) to remove.

Defaults The permitted vendor list is empty by default and all vendors are allowed. However, after you add an entry to the list, UNIVERGE WL Control System allows only the devices whose OUIs are on the list.

Access Enabled.

Usage The permitted vendor list applies only to the UNIVERGE WL Controller on which the list is configured. UNIVERGE WL Controllers do not share permitted vendor lists.

If you add a device that UNIVERGE WL Control System has classified as a rogue to the permitted vendor list, but not to the ignore list, UNIVERGE WL Control System can still classify the device as a rogue. Adding an entry to the permitted vendor list merely indicates that the device is from an allowed vendor. However, to cause UNIVERGE WL Control System to stop classifying the device as a rogue, you must add the device's MAC address to the ignore list.

Examples The following command adds an entry for clients whose MAC addresses start with aa:bb:cc:

```
PROMPT# set rfdetect vendor-list client aa:bb:cc:00:00:00
success: MAC aa:bb:cc:00:00:00 is now in client vendor-list.
```

The trailing 00:00:00 value is required.

See Also

- 1 **clear rfdetect vendor-list** on page 550
- 1 **show rfdetect vendor-list** on page 573

show rfdetect attack-list

Displays information about the MAC addresses in the attack list.

Syntax **show rfdetect attack-list**

Defaults None.

Access Enabled.

Examples The following example shows the attack list on UNIVERGE WL Controller:

```
PROPMT# show rfdetect attack-list
Total number of entries: 1
Attacklist MAC      Port/Radio/Chan  RSSI      SSID
-----
11:22:33:44:55:66  ap 2/1/11       -53       rogue-ssid
```

See Also

- 1 **clear rfdetect attack-list** on page 548
- 1 **set rfdetect attack-list** on page 552

show rfdetect black-list

Displays information about the clients in the client black list.

Syntax **show rfdetect black-list**

Defaults None.

Access Enabled.

show rfdetect clients

Chapter 19

Examples The following example shows the client black list on UNIVERGE WL Controller:

```
PROPMT# show rfdetect black-list
Total number of entries: 1
  Blacklist MAC      Type      Port  TTL
-----
11:22:33:44:55:66 configured -      -
11:23:34:45:56:67 assoc req flood 3      25
```

See Also

- 1 **clear rfdetect black-list** on page 549
- 1 **set rfdetect black-list** on page 553

show rfdetect clients

Displays the wireless clients detected by a UNIVERGE WL Controller.

Syntax **show rfdetect clients** [**mac** *mac-addr*]

mac *mac-addr* Displays detailed information for a specific client.

Defaults None.

Access Enabled.

Examples The following command shows information about all wireless clients detected by a UNIVERGE WL Access Point:

```
PROPMT# show rfdetect clients
Total number of entries: 30
Client MAC      Client      AP MAC      AP      Port/Radio      NoL Type      Last
                Vendor      Vendor      Vendor      /Channel
-----
00:03:7f:bf:16:70 Unknown      Unknown      ap 1/1/6      1 intfr 207
00:04:23:77:e6:e5 Intel         Unknown      ap 1/1/2      1 intfr 155
00:05:5d:79:ce:0f D-Link        Unknown      ap 1/1/149    1 intfr 87
00:05:5d:7e:96:a7 D-Link        Unknown      ap 1/1/149    1 intfr 117
00:05:5d:7e:96:ce D-Link        Unknown      ap 1/1/157    1 intfr 162
00:05:5d:84:d1:c5 D-Link        Unknown      ap 1/1/1      1 intfr 52
```

The following command displays more details about a specific client:

```

PROPMT# show rfdetect clients mac 00:0c:41:63:fd:6d
Client Mac Address: 00:0c:41:63:fd:6d, Vendor: Linksys
Port: ap 1, Radio: 1, Channel: 11, RSSI: -82, Rate: 2, Last Seen (secs ago): 84
Bssid: 00:0b:0e:01:02:00, Vendor: NEC, Type: intfrr, Dst: ff:ff:ff:ff:ff:ff
Last Rogue Status Check (secs ago): 3

```

The first line lists information for the client. The other lines list information about the most recent 802.11 packet detected from the client.

Table 68 and Table 69 describe the fields in these displays.

Table 68. show rfdetect clients Output

Field	Description
Client MAC	MAC address of the client.
Client Vendor	Company that manufactures or sells the client.
AP MAC	MAC address of the radio with which the rogue client is associated.
AP Vendor	Company that manufactures or sells the AP with which the rogue client is associated.
Port/Radio/Channel	AP number, radio number, and channel number of the radio that detected the rogue.
NoL	Number of listeners. This is the number of UNIVERGE WL Access Points radios that detected the rogue client.

Table 68. show rfdetect clients Output

Field	Description
Type	Classification of the rogue device: <ul style="list-style-type: none">• rogue—Wireless device that is on the network but is not supposed to be on the network.• infr—Wireless device that is not part of your network and is not a rogue, but might be causing RF interference with UNIVERGE WL Access Points radios.• known—Device that is a legitimate member of the network.
Last seen	Number of seconds since a UNIVERGE WL Access Points radio last detected 802.11 packets from the device.

Table 69. show rfdetect clients mac Output

Field	Description
RSSI	Received signal strength indication (RSSI)—the strength of the RF signal detected by the AP radio, in decibels referred to 1 milliwatt (dBm).
Rate	The data rate of the client.
Last Seen	Number of seconds since a UNIVERGE WL Access Point radio last detected 802.11 packets from the device.
BSSID	MAC address of the SSID with which the rogue client is associated.
Vendor	Company that manufactures or sells the AP with which the rogue client is associated.

Table 69. show rfdetect clients mac Output

Field	Description
Typ	Classification of the rogue device: <ul style="list-style-type: none">• rogue—Wireless device that is on the network but is not supposed to be on the network.• infr—Wireless device that is not part of your network and is not a rogue, but might be causing RF interference with UNIVERGE WL Access Points radios.• known—Device that is a legitimate member of the network.
Dst	MAC addressed to which the last 802.11 packet detected from the client was addressed.
Last Rogue Status Check	Number of seconds since the UNIVERGE WL Controller looked on the air for the AP with which the rogue client is associated. The UNIVERGE WL Controller looks for the client's AP by sending a packet from the wired side of the network addressed to the client, and watching the air for a wireless packet containing the client's MAC address.

show rfdetect countermeasures

Displays the current status of countermeasures against rogues in the Mobility Domain.

Syntax show rfdetect countermeasures

Defaults None.

Access Enabled.

Usage This command is valid only on the seed UNIVERGE WL Controller of the Mobility Domain.

Examples The following example displays countermeasures status for the Mobility Domain:

show rfdetect counters

Chapter 19

```
PROPMT# show rfdetect countermeasures
Total number of entries: 190
Rogue MAC          Type  Countermeasures  Switch-IPaddr  Port/Radio
                   Radio Mac                                     /Channel
-----
00:0b:0e:00:71:c0  intfr 00:0b:0e:44:55:66  10.1.1.23      ap 4/1/6
00:0b:0e:03:00:80  rogue 00:0b:0e:11:22:33  10.1.1.23      ap 2/1/11
```

Table 70 describes the fields in this display.

Table 70. show rfdetect countermeasures Output

Field	Description
Rogue MAC	BSSID of the rogue.
Type	Classification of the rogue device: <ul style="list-style-type: none">• rogue—Wireless device that is on the network but is not supposed to be on the network.• intfr—Wireless device that is not part of your network and is not a rogue, but might be causing RF interference with UNIVERGE WL Access Points radios.• known—Device that is a legitimate member of the network.
Countermeasures Radio MAC	MAC address of the UNIVERGE WL Access Points radio sending countermeasures against the rogue.
Switch-IPaddr	System IP address of the UNIVERGE WL Controller that is managing the UNIVERGE WL Access Points that is sending or will send countermeasures.
Port/Radio/Channel	AP number, radio number, and channel number of the countermeasures radio.

See Also set radio-profile countermeasures on page 307

show rfdetect counters

Displays statistics for rogue and Intrusion Detection System (IDS) activity detected by the UNIVERGE WL Access Points managed by a UNIVERGE WL Controller.

Syntax show rfdetect counters

Defaults None.

Access Enabled.

Examples The following command shows counters for rogue activity detected by a UNIVERGE WL Controller:

```

PROPMT# show rfdetect counters
Type                               Current      Total
-----
Rogue access points                0            0
Interfering access points          139          1116
Rogue 802.11 clients                0            0
Interfering 802.11 clients          4            347
802.11 adhoc clients                0            1
Unknown 802.11 clients              20           965
Interfering 802.11 clients seen on wired network 0            0
802.11 probe request flood          0            0
802.11 authentication flood         0            0
802.11 null data flood              0            0
802.11 mgmt type 6 flood            0            0
802.11 mgmt type 7 flood            0            0
802.11 mgmt type d flood            0            0
802.11 mgmt type e flood            0            0
802.11 mgmt type f flood            0            0
802.11 association flood            0            0
802.11 reassociation flood          0            0
802.11 disassociation flood         0            0
Weak wep initialization vectors      0            0
Spoofed access point mac-address attacks 0            0
Spoofed client mac-address attacks  0            0
Ssid masquerade attacks             1            12
Spoofed deauthentication attacks     0            0
Spoofed disassociation attacks       0            0
Null probe responses                626          11380
Broadcast deauthentications          0            0
FakeAP ssid attacks                 0            0
FakeAP bssid attacks                 0            0
Netstumbler clients                  0            0
Wellenreiter clients                0            0
Active scans                         1796          4383
Wireless bridge frames               196           196
Adhoc client frames                  8             0
Access points present in attack-list 0            0
Access points not present in ssid-list 0            0
Access points not present in vendor-list 0            0
Clients not present in vendor-list   0            0
Clients added to automatic black-list 0            0

```

show rfdetect data

Displays information about the APs detected by a UNIVERGE WL Controller.

Syntax `show rfdetect data`

Defaults None.

Access Enabled.

Usage You can enter this command on any UNIVERGE WL Controller in the Mobility Domain. The output applies only to the UNIVERGE WL Controller on which you enter the command. To display all devices that a specific UNIVERGE WL Access Points radio has detected, even if the radio is managed by another UNIVERGE WL Controller, use the **show rfdetect visible** command.

To display rogue information for the entire Mobility Domain, use the **show rfdetect mobility-domain** command on the seed UNIVERGE WL Controller.

Only one MAC address is listed for each UNIVERGE WL Access Points radio, even if the radio is beaconing multiple SSIDs.

Examples The following command shows the devices detected by this UNIVERGE WL Controller during the most recent RF detection scan:

```

PROPMT# show rfdetect data
Total number of entries: 197
Flags: i = infrastructure, a = ad-hoc
       c = CCMP, t = TKIP, l = 104-bit WEP, 4 = 40-bit WEP, w = WEP(non-WPA)
BSSID      Vendor  Type  Port/Radio/Ch  Flags  RSSI  Age  SSID
-----
00:07:50:d5:cc:91  Cisco  intfr      3/1/6  i---w  -61   6  r27-cisco1200-2
00:07:50:d5:dc:78  Cisco  intfr      3/1/6  i---w  -82   6  r116-cisco1200-2
00:09:b7:7b:8a:54  Cisco  intfr      3/1/2  i-----  -57   6
00:0a:5e:4b:4a:c0  3Com   intfr      3/1/11 i-----  -57   6  public
00:0a:5e:4b:4a:c2  3Com   intfr      3/1/11 i-t1--  -86   6  wlan
00:0a:5e:4b:4a:c4  3Com   intfr      3/1/11 ic----  -85   6  ccmp
00:0a:5e:4b:4a:c6  3Com   intfr      3/1/11 i-t---  -85   6  tkip
00:0a:5e:4b:4a:c8  3Com   intfr      3/1/11 i---w  -83   6  -voip
00:0a:5e:4b:4a:ca  3Com   intfr      3/1/11 i-----  -85   6  webaaa
...

```

Table 71 describes the fields in this display.

Table 71. show rfdetect data Output

Field	Description
Field	Description
BSSID	MAC address of the SSID used by the detected device.
Vendor	Company that manufactures or sells the rogue device.
Type	Classification of the rogue device: <ul style="list-style-type: none"> • rogue—Wireless device that is not supposed to be on the network. The device has an entry in a UNIVERGE WL Controller FDB and is therefore on the network. • intfr—Wireless device that is not part of your network but is not a rogue. The device does not have an entry in a UNIVERGE WL Controller FDB and is not actually on the network, but might be causing RF interference with UNIVERGE WL Access Points radios. • known—Device that is a legitimate member of the network.
Port/Radio/Channel	AP number, radio number, and channel number of the radio that detected the rogue.
Flags	Classification and encryption information for the rogue: <ul style="list-style-type: none"> • The i, a, or u flag indicates the classification. • The other flags indicate the encryption used by the rogue. For flag definitions, see the key in the command output.
RSSI	Received signal strength indication (RSSI)—the strength of the RF signal detected by the AP radio, in decibels referred to 1 milliwatt (dBm).
Age	Number of seconds since n UNIVERGE WL Access Point radio last detected 802.11 packets from the device.

See Also

- 1 **show rfdetect mobility-domain** on page 568
- 1 **show rfdetect visible** on page 574

show rfdetect ignore

Displays the BSSIDs of third-party devices that UNIVERGE WL Control System ignores during RF scans. UNIVERGE WL Control System does not generate log messages or traps for the devices in the ignore list.

Syntax **show rfdetect ignore**

Defaults None.

Access Enabled.

Examples The following example displays the list of ignored devices:

```
PROPMT# show rfdetect ignore
Total number of entries: 2
  Ignore MAC
  -----
aa:bb:cc:11:22:33
aa:bb:cc:44:55:66
```

See Also

1 **clear rfdetect ignore** on page 549

1 **set rfdetect ignore** on page 554

show rfdetect mobility-domain

Displays the rogues detected by all UNIVERGE WL Controllers in the Mobility Domain during RF detection scans.

Syntax **show rfdetect mobility-domain**
[**ssid** *ssid-name* | **bssid** *mac-addr*]

ssid *ssid-name* Displays rogues that are using the specified SSID.

bssid *mac-addr* Displays rogues that are using the specified BSSID.

Defaults None.

Access Enabled.

Usage This command is valid only on the seed UNIVERGE WL Controller of the Mobility Domain. To display rogue information for an individual UNIVERGE WL Controller, use the **show rfdetect data** command on that UNIVERGE WL Controller.

Examples The following command displays summary information for all SSIDs and BSSIDs detected in the Mobility Domain:

```

PROPMT# show rfdetect mobility-domain
Total number of entries: 194
Flags: i = infrastructure, a = ad-hoc, u = unresolved
       c = CCMP, t = TKIP, 1 = 104-bit WEP, 4 = 40-bit WEP, w = WEP(non-WPA)
BSSID      Vendor      Type  Flags  SSID
-----
00:07:50:d5:cc:91    Cisco intfr i----w r27-cisco1200-2
00:07:50:d5:dc:78    Cisco intfr i----w r116-cisco1200-2
00:09:b7:7b:8a:54    Cisco intfr i-----
00:0a:5e:4b:4a:c0     3Com intfr i----- public
00:0a:5e:4b:4a:c2     3Com intfr i----w wlan
00:0a:5e:4b:4a:c4     3Com intfr ic---- ccmp
00:0a:5e:4b:4a:c6     3Com intfr i----w tkip
00:0a:5e:4b:4a:c8     3Com intfr i----w voip
00:0a:5e:4b:4a:ca     3Com intfr i----- webaaa
...

```

The lines in this display are compiled from data from multiple listeners (UNIVERGE WL Access Points radios). If an item has the value *unresolved*, not all listeners agree on the value for that item. Generally, an unresolved state occurs only when a UNIVERGE WL Access Point or a Mobility Domain is still coming up, and lasts only briefly.

The following command displays detailed information for rogues using SSID *webaaa*.

```

PROPMT# show rfdetect mobility-domain ssid webaaa
BSSID: 00:0a:5e:4b:4a:ca Vendor: 3Com SSID: webaaa
Type: intfr Adhoc: no Crypto-types: clear

Switch-IPaddress: 10.8.121.102 Port/Radio/Ch: 3/1/11 Mac: 00:0b:0e:00:0a:6a
Device-type: interfering Adhoc: no Crypto-types: clear
RSSI: -85 SSID: webaaa

BSSID: 00:0b:0e:00:7a:8a Vendor: NEC SSID: webaaa
Type: intfr Adhoc: no Crypto-types: clear

Switch-IPaddress: 10.8.121.102 Port/Radio/Ch: 3/1/1 Mac: 00:0b:0e:00:0a:6a
Device-type: interfering Adhoc: no Crypto-types: clear
RSSI: -75 SSID: webaaa

```

show rfdetect mobility-domain

Chapter 19

```
Switch-IPaddress: 10.3.8.103 Port/Radio/Ch: ap 1/1/1 Mac: 00:0b:0e:76:56:82
Device-type: interfering Adhoc: no Crypto-types: clear
RSSI: -76 SSID: webaaa
```

Two types of information are shown. The lines that are not indented show the BSSID, vendor, and information about the SSID. The indented lines that follow this information indicate the listeners (UNIVERGE WL Access Points radios) that detected the SSID. Each set of indented lines is for a separate UNIVERGE WL Access Points listener.

In this example, two BSSIDs are mapped to the SSID. Separate sets of information are shown for each of the BSSIDs, and information about the listeners for each BSSID is shown.

The following command displays detailed information for a BSSID.

```
PROPM# show rfdetect mobility-domain bssid 00:0b:0e:00:04:d1
BSSID: 00:0b:0e:00:04:d1 Vendor: Cisco SSID: notmycorp
Type: rogue Adhoc: no Crypto-types: clear

Switch-IPaddress: 10.8.121.102 Port/Radio/Ch: 3/2/56 Mac: 00:0b:0e:00:0a:6b
Device-type: rogue Adhoc: no Crypto-types: clear
RSSI: -72 SSID: notmycorp

Switch-IPaddress: 10.3.8.103 Port/Radio/Ch: ap 1/1/157 Mac: 00:0b:0e:76:56:82
Device-type: rogue Adhoc: no Crypto-types: clear
RSSI: -72 SSID: notmycorp
```

Table 72 and Table 73 describe the fields in these displays.

Table 72. show rfdetect mobility-domain Output

Field	Description
BSSID	MAC address of the SSID used by the detected device.
Vendor	Company that manufactures or sells the rogue device.
Type	Classification of the rogue device: <ul style="list-style-type: none"> • rogue—Wireless device that is not supposed to be on the network. The device has an entry in a UNIVERGE WL Controller FDB and is therefore on the network. • infr—Wireless device that is not part of your network but is not a rogue. The device does not have an entry in a UNIVERGE WL Controller FDB and is not actually on the network, but might be causing RF interference with UNIVERGE WL Access Points radios. • known—Device that is a legitimate member of the network.
Flags	Classification and encryption information for the rogue: <ul style="list-style-type: none"> • The i, a, or u flag indicates the classification. • The other flags indicate the encryption used by the rogue. For flag definitions, see the key in the command output.
SSID	SSID used by the detected device.

Table 73. show rfdetect mobility-domain ssid or bssid Output

Field	Description
BSSID	MAC address of the SSID used by the detected device.
Vendor	Company that manufactures or sells the rogue device.
SSID	SSID used by the detected device.

Table 73. show rfdetect mobility-domain ssid or bssid Output

Field	Description
Type	Classification of the rogue device: <ul style="list-style-type: none"> • rogue—Wireless device that is on the network but is not supposed to be on the network. • infr—Wireless device that is not part of your network and is not a rogue, but might be causing RF interference with UNIVERGE WL Access Points radios. • known—Device that is a legitimate member of the network.
Adhoc	Indicates whether the rogue is an infrastructure rogue (is using an AP) or is operating in ad-hoc mode.
Crypto-Types	Encryption type: <ul style="list-style-type: none"> • clear (no encryption) • ccmp • tkip • wep104 (WPA 104-bit WEP) • wep40 (WPA 40-bit WEP) • wep (non-WPA WEP)
Switch-IPaddress	System IP address of the UNIVERGE WL Controller that detected the rogue.
Port/Radio/Channel	AP number, radio number, and channel number of the radio that detected the rogue.
Mac	MAC address of the radio that detected the rogue.
Device-type	Device type detected by the UNIVERGE WL Access Points radio.
Adhoc	Ad-hoc status (yes or no) detected by the UNIVERGE WL Access Points radio.
Crypto-Types	Encryption type detected by the UNIVERGE WL Access Points radio.
RSSI	Received signal strength indication (RSSI)—the strength of the RF signal detected by the AP radio, in decibels referred to 1 milliwatt (dBm).

Table 73. show rfdetect mobility-domain ssid or bssid Output

Field	Description
SSID	SSID mapped to the BSSID.

See Also

- 1 **show rfdetect data** on page 566
- 1 **show rfdetect visible** on page 574

show rfdetect ssid-list

Displays the entries in the permitted SSID list.

Syntax **show rfdetect ssid-list**

Defaults None.

Access Enabled.

Examples The following example shows the permitted SSID list on UNIVERGE WL Controller:

```
PROPMT# show rfdetect ssid-list
Total number of entries: 3
      SSID
-----
      mycorp
      corporate
      guest
```

See Also

- 1 **clear rfdetect ssid-list** on page 550
- 1 **set rfdetect ssid-list** on page 557

show rfdetect vendor-list

Displays the entries in the permitted vendor list.

show rfdetect visible

Chapter 19

Syntax **show rfdetect vendor-list**

Defaults None.

Access Enabled.

Examples The following example shows the permitted vendor list on UNIVERGE WL Controller:

```
PROPMT# show rfdetect vendor-list
Total number of entries: 1
      OUI          Type
-----
aa:bb:cc:00:00:00 client
11:22:33:00:00:00 client
```

See Also

- 1 **clear rfdetect vendor-list** on page 550
- 1 **set rfdetect vendor-list** on page 558

show rfdetect visible

Displays the BSSIDs discovered by a specific UNIVERGE WL Access Points radio.

Syntax **show rfdetect visible** *mac-addr*

Syntax **show rfdetect visible ap** *ap-number* [**radio** {**1** | **2**}]

mac-addr Base MAC address of the UNIVERGE WL Access Points radio.

Note: To display the base MAC address of a UNIVERGE WL Access Points radio, use the **show ap status** command.

ap-number Number of a UNIVERGE WL Access Points for which to display neighboring BSSIDs.

radio 1 Shows neighbor information for radio 1.

radio 2 Shows neighbor information for radio 2. (This option does not apply to single-radio models.)

Defaults None.

Access Enabled.

Usage If a UNIVERGE WL Access Points radio is supporting more than one SSID, each of the corresponding BSSIDs is listed separately.

To display rogue information for the entire Mobility Domain, use the **show rfdetect mobility-domain** command on the seed UNIVERGE WL Controller.

Examples To following command displays information about the rogues detected by radio 1 on UNIVERGE WL Access Points 3:

```

PROPMT# show rfdetect visible ap 3 radio 1
Total number of entries: 104
Flags: i = infrastructure, a = ad-hoc
       c = CCMP, t = TKIP, l = 104-bit WEP, 4 = 40-bit WEP, w = WEP(non-WPA)
Transmit MAC      Vendor  Type  Ch  RSSI  Flags  SSID
-----
00:07:50:d5:cc:91  Cisco  intf  6   -60  i---w  r27-cisco1200-2
00:07:50:d5:dc:78  Cisco  intf  6   -82  i---w  r116-cisco1200-2
00:09:b7:7b:8a:54  Cisco  intf  2   -54  i-----
00:0a:5e:4b:4a:c0  3Com  intf  11  -57  i----- public
00:0a:5e:4b:4a:c2  3Com  intf  11  -86  i-t1-- univergewlan
00:0a:5e:4b:4a:c4  3Com  intf  11  -85  ic---- unvg-ccmp
00:0a:5e:4b:4a:c6  3Com  intf  11  -85  i-t--- unvg-tkip
00:0a:5e:4b:4a:c8  3Com  intf  11  -83  i---w  unvg-voip
00:0a:5e:4b:4a:ca  3Com  intf  11  -85  i----- unvg-webaaa
...

```

Table 74 describes the fields in this display.

Table 74. show rfdetect visible Output

Field	Description
Transmit MAC	MAC address the rogue device that sent the 802.11 packet detected by the UNIVERGE WL Access Points radio.
Vendor	Company that manufactures or sells the rogue device.
Type	Classification of the rogue device: <ul style="list-style-type: none">• rogue—Wireless device that is on the network but is not supposed to be on the network.• intfr—Wireless device that is not part of your network and is not a rogue, but might be causing RF interference with UNIVERGE WL Access Points radios.• known—Device that is a legitimate member of the network.
Ch	Channel number on which the radio detected the rogue.
RSSI	Received signal strength indication (RSSI)—the strength of the RF signal detected by the AP radio, in decibels referred to 1 milliwatt (dBm).
Flags	Classification and encryption information for the rogue: <ul style="list-style-type: none">• The i, a, or u flag indicates the classification.• The other flags indicate the encryption used by the rogue. For flag definitions, see the key in the command output.
SSID	SSID used by the detected device.

See Also

- 1 **show rfdetect data** on page 566
- 1 **show rfdetect mobility-domain** on page 568

File Management Commands

Use file management commands to manage system files and to display software and boot information. This chapter presents file management commands alphabetically. Use the following table to locate commands in this chapter based on their use.

Software Version	reset system on page 591
	show version on page 602
Boot Settings	set boot partition on page 597
	set boot configuration-file on page 596
	set boot backup-configuration on page 595
	show boot on page 597
	clear boot config on page 580
File Management	clear boot backup-configuration on page 579
	dir on page 584
	copy on page 581
	md5 on page 589
	delete on page 583
	mkdir on page 589
	rmdir on page 594
Configuration File	save config on page 594
	load config on page 587
	show config on page 600

System Backup and Restore

backup on page 578

restore on page 592

backup

Creates an archive of UNIVERGE WL Control system files and optionally, user file, in Unix *tape archive (tar)* format.

Syntax **backup system** [**tftp:/ip-addr/**]*filename* [**all** | **critical**]

[**tftp:/ip-addr/**]*filename*

Name of the archive file to create. You can store the file locally in the UNIVERGE WL Controllers nonvolatile storage or on a TFTP server.

all

Backs up system files and all the files in the user files area.

The user files area contains the set of files listed in the *file* section of **dir** command output.

critical

Backs up system files only, including the configuration file used when booting, and certificate files. The size of an archive created by this option is generally 1MB or less.

Defaults The default is **all**.

Access Enabled.

Usage You can create an archive located on a TFTP server or in the UNIVERGE WL Controllers nonvolatile storage. If you specify a TFTP server as part of the filename, the archive is copied directly to the TFTP server and not stored locally on the UNIVERGE WL Controller.

Use the **critical** option if you want to back up or restore only the system-critical files required to operate and communicate with the UNIVERGE WL Controller. Use the **all** option if you also want to back up or restore Web Authentication pages, backup configuration files, image files, and any other files stored in the user files area of nonvolatile storage.

The maximum supported file size is 32 MB. If the file size of the tarball is too large, delete unnecessary files (such as unneeded copies of system image files) and try again, or use the **critical** option instead of the **all** option.

Neither option archives image files or any other files listed in the *Boot* section of **dir** command output. The **all** option archives image files only if they are present in the user files area.

Archive files created by the **all** option are larger than files created by the **critical** option. The file size depends on the files in the user area, and the file can be quite large if the user area contains image files.

The **backup** command places the boot configuration file into the archive. (The boot configuration file is the *Configured boot configuration* in the **show boot** command's output.) If the running configuration contains changes that have not been saved, these changes are not in the boot configuration file and are not archived. To make sure the archive contains the configuration that is currently running on the UNIVERGE WL Controller, use the **save config** command to save the running configuration to the boot configuration file, before using the **backup** command.

Examples The following command creates an archive of the system-critical files and copies the archive directly to a TFTP server. The filename in this example includes a TFTP server IP address, so the archive is not stored locally on the UNIVERGE WL Controller.

```
PROMPT# backup system tftp://10.10.20.9/sysa_bak critical
success: sent 13082 bytes in 0.052 seconds [ 251576 bytes/sec]

success: received 13082 bytes in 0.227 seconds [ 57629 bytes/sec]

success: backup complete.
```

See Also

- 1 **dir** on page 584
- 1 **restore** on page 592

clear boot backup-configuration

Clears the filename specified as the backup configuration file. In the event that UNIVERGE WL Control System cannot read the configuration file at boot time, a backup configuration file is not used.

Syntax `clear boot backup-configuration`

Defaults None.

Access Enabled.

Examples The following command clears the name specified as the backup configuration file from the configuration of the UNIVERGE WL Controller:

```
PROMPT# clear boot backup-configuration
success: Backup boot config filename was cleared.
```

See Also

- 1 **set boot backup-configuration** on page 595
- 1 **show boot** on page 597

clear boot config

Resets to the factory default the configuration that UNIVERGE WL Control System loads during a reboot.

Syntax `clear boot config`

Defaults None.

Access Enabled.

Examples The following commands back up the configuration file on a UNIVERGE WL Controller, reset the UNIVERGE WL Controller to its factory default configuration, and reboot the UNIVERGE WL Controller:

```
PROMPT# copy configuration tftp://10.1.1.1/backupcfg
success: sent 365 bytes in 0.401 seconds [ 910 bytes/sec]
```

```
PROMPT# clear boot config
success: Reset boot config to factory defaults.
```

```
PROMPT# reset system force
```

See Also

- 1 **reset system** on page 591
- 1 **show config** on page 600

copy

Performs the following copy operations:

- 1 Copies a file from a TFTP server to nonvolatile storage.
- 1 Copies a file from nonvolatile storage or temporary storage to a TFTP server.
- 1 Copies a file from one area in nonvolatile storage to another.
- 1 Copies a file to a new filename in nonvolatile storage.

Syntax **copy** *source-url destination-url*

source-url Name and location of the file to copy. The uniform resource locator (URL) can be one of the following:

- *[subdirname/]filename*
- **file:***[subdirname/]filename*
- **tftp://ip-addr/***[subdirname/]filename*
- **tmp:***filename*

For the filename, specify between 1 and 128 alphanumeric characters, with no spaces. Enter the IP address in dotted decimal notation.

The *subdirname/* option specifies a subdirectory.

destination-url Name of the copy and the location where to place the copy. The URL can be one of the following:

- *[subdirname/]filename*
- **file:***[subdirname/]filename*
- **tftp://ip-addr/***[subdirname/]filename*

If you are copying a system image file into nonvolatile storage, the filename must include the boot partition name. You can specify one of the following:

- **boot0:***filename*
- **boot1:***filename*

Defaults None.

Access Enabled.

Usage The *filename* and **file:filename** URLs are equivalent. You can use either URL to refer to a file in a UNIVERGE WL Controller nonvolatile memory. The **tftp://ip-addr/filename** URL refers to a file on a TFTP server. If DNS is configured on the UNIVERGE WL Controller, you can specify a TFTP server's hostname as an alternative to specifying the IP address.

The **tmp:filename** URL specifies a file in temporary storage. You can copy a file out of temporary storage but you cannot copy a file into temporary storage. Temporary storage is reserved for use by UNIVERGE WL Control System.

If you are copying a system image file into nonvolatile storage, the filename must be preceded by the boot partition name, which can be **boot0** or **boot1**. Enter the filename as **boot0:filename** or **boot1:filename**. You must specify the boot partition that *was not* used to load the currently running image.

The maximum supported file size for TFTP is 32 MB.

Examples The following command copies a file called *floorwl* from nonvolatile storage to a TFTP server:

```
PROMPT# copy floorwl tftp://10.1.1.1/floorwl
success: sent 365 bytes in 0.401 seconds [ 910 bytes/sec]

success: copy complete.
```

The following command copies a file called *closetwl* from a TFTP server to nonvolatile storage:

```
PROMPT# copy tftp://10.1.1.1/closetwl closetwl
success: received 637 bytes in 0.253 seconds [ 2517 bytes/sec]

success: copy complete.
```

The following command copies system image *UV04240.021* from a TFTP server to boot partition 1 in nonvolatile storage:

```
PROMPT# copy tftp://10.1.1.107/UV04240.021 boot1:UV04240.021
.....
.....success: received 9163214 bytes in 105.939 seconds
[ 86495 bytes/sec]

success: copy complete.
```

The following commands rename *test-config* to *new-config* by copying it from one name to the other in the same location, then deleting *test-config*:

```
PROMPT# copy test-config new-config
PROMPT# delete test-config
success: file deleted.
```

The following command copies file *corpa-login.html* from a TFTP server into subdirectory *corpa* in a UNIVERGE WL Controller nonvolatile storage:

```
PROMPT# copy tftp://10.1.1.1/corpa-login.html corpa/corpa-login.html
success: received 637 bytes in 0.253 seconds [ 2517 bytes/sec]
```

```
success: copy complete.
```

See Also

1 **delete** on page 583

1 **dir** on page 584

delete

Deletes a file.



Caution! UNIVERGE WL Control System does not prompt you to verify whether you want to delete a file. When you press Enter after typing a **delete** command, UNIVERGE WL Control System immediately deletes the specified file.



Note. UNIVERGE WL Control System does not allow you to delete the currently running software image file or the running configuration.

Syntax `delete url`

url Filename. Specify between 1 and 128 alphanumeric characters, with no spaces.
If the file is in a subdirectory, specify the subdirectory name, followed by a forward slash, in front of the filename.
For example: **subdir_a/file_a**.

Defaults None.

Access Enabled.

Usage You might want to copy the file to a TFTP server as a backup before deleting the file.

Examples The following commands copy file *testconfig* to a TFTP server and delete the file from nonvolatile storage:

```
PROMPT# copy testconfig tftp://10.1.1.1/testconfig
success: sent 365 bytes in 0.401 seconds [ 910 bytes/sec]
```

```
success: copy complete.
```

```
PROMPT# delete testconfig
success: file deleted.
```

Examples The following command deletes file *dang_doc* from subdirectory *dang*:

```
PROMPT# delete dang/dang_doc
success: file deleted.
```

See Also

- 1 **copy** on page 581
- 1 **dir** on page 584

dir

Displays a list of the files in nonvolatile storage and temporary files.

Syntax **dir** [*subdirname*] | [**file:**] | [**core:**] | [**boot0:**] | [**boot1:**]

subdirname Subdirectory name. If you specify a subdirectory name, the command lists the files in that subdirectory. Otherwise, the command lists the files in the root directory and also lists the subdirectories.

file: Limits **dir** output to the contents of the user files area

core: Limits **dir** output to the contents of the */tmp/core* subdirectory

boot0: Limits **dir** output to the contents of the *boot0* partition

boot1: Limits **dir** output to the contents of the *boot1* partition

Defaults None.

Access Enabled.

Examples The following command displays the files in the root directory:

```
PROMPT# dir
=====
file:
Filename                               Size           Created
file:configuration                     13 KB          Dec 28 2006, 09:55:54
file:qs_template.xml                   13 KB          Feb 08 2007, 16:33:33
Total:                                26 Kbytes used, 84516 Kbytes free
=====
Boot:
Filename                               Size           Created
boot0:SR060200.002                     8092 KB        Jan 23 2007, 15:51:02
*boot1:SR060200.003                     8103 KB        Feb 05 2007, 19:35:47
Boot0: Total:                          8092 Kbytes used, 9166 Kbytes free
Boot1: Total:                          8103 Kbytes used, 9156 Kbytes free
=====
temporary files:
Filename                               Size           Created
core:command_audit.cur                  159 KB          Feb 08 2007, 16:33:33
core:command_audit.pre                   500 KB          Mar 03 1988, 23:52:03
Total:                                659 Kbytes used, 83908 Kbytes free
```

The following command displays the files in the *old* subdirectory:

dir

Chapter 20

PROMPT# dir old

```
=====
file:
Filename                               Size          Created
file:configuration.txt                 3541 bytes    Sep 22 2003, 22:55:44
file:configuration.xml                  24 KB        Sep 22 2003, 22:55:44
Total:                                27 Kbytes used, 207824 Kbytes free
```

The following command limits the output to the contents of the user files area:

PROMPT# dir file:

```
=====
file:
Filename                               Size          Created
file:configuration                     48 KB        Jul 12 2005, 15:02:32
file:corp2:corp2cnfig                  17 KB        Mar 14 2005, 22:20:04
corp_a/                                512 bytes    May 21 2004, 19:15:48
file:dangcfg                            14 KB        Mar 14 2005, 22:20:04
dangdir/                                512 bytes    May 16 2004, 17:23:44
file:pubsconfig-april062005            40 KB        May 09 2005, 21:08:30
file:sysa_bak                           12 KB        Mar 15 2005, 19:18:44
file:testback                           28 KB        Apr 19 2005, 16:37:18
Total:                                159 Kbytes used, 207663 Kbytes free
```

The following command limits the output to the contents of the */tmp/core* subdirectory:

PROMPT# dir core:

```
=====
file:
Filename                               Size          Created
core:command_audit.cur                 37 bytes      Aug 28 2005, 21:11:41
Total:                                  37 bytes used, 91707 Kbytes free
```

The following command limits the output to the contents of the *boot0* partition:

PROMPT# dir boot0:

```
=====
file:
Filename                               Size          Created
boot0:SC060200.002                     8092 KB       Jan 23 2007, 15:51:02
Total:                                8092 Kbytes used, 9166 Kbytes free
```

Table 75 describes the fields in the **dir** output.

Table 75. Output for dir

Field	Description
Filename	Filename or subdirectory name. For files, the directory name is shown in front of the filename (for example, file:configuration). The <i>file:</i> directory is the root directory. For subdirectories, a forward slash is shown at the end of the subdirectory name (for example, old/). In the boot partitions list (Boot:), an asterisk (*) indicates the boot partition from which the currently running image was loaded and the image filename.
Size	Size in Kbytes or bytes.
Created	System time and date when the file was created or copied onto the UNIVERGE WL Controller.
Total	Number of kilobytes in use to store files and the number that are still free.

See Also

- 1 **copy** on page 581
- 1 **delete** on page 583

load config



Caution! This command completely removes the running configuration and replaces it with the configuration contained in the file. UNIVERGE WL Control System recommends that you save a copy of the current running configuration to a backup configuration file before loading a new configuration.

Loads configuration commands from a file and replaces the UNIVERGE WL Controllers running configuration with the commands in the loaded file.

Syntax **load config** [*url*]

url Filename. Specify between 1 and 128 alphanumeric characters, with no spaces.
If the file is in a subdirectory, specify the subdirectory name, followed by a forward slash, in front of the filename.
For example: **backup_configs/config_c**.

Defaults The default file location is nonvolatile storage.



Note. UNIVERGE WL Control System supports loading a configuration file only from the UNIVERGE WL Controllers nonvolatile storage. You cannot load a configuration file directly from a TFTP server.

If you do not specify a filename, UNIVERGE WL Control System uses the same configuration filename that was used for the previous configuration load. For example, if the UNIVERGE WL Controller used *configuration* for the most recent configuration load, UNIVERGE WL Control System uses *configuration* again unless you specify a different filename. To display the filename of the configuration file UNIVERGE WL Control System loaded during the last reboot, use the **show boot** command.

Access Enabled.

Usage This command completely replaces the running configuration with the configuration in the file.

Examples The following command reloads the configuration from the most recently loaded configuration file:

```
PROMPT# load config
Reloading configuration may result in lost of connectivity, do you wish to
continue? (y/n) [n]y
success: Configuration reloaded
```

The following command loads configuration file *testconfig1*:

```
PROMPT# load config testconfig1
Reloading configuration may result in lost of connectivity, do you wish to
continue? (y/n) [n]y
success: Configuration reloaded
```

See Also

- 1 **save config** on page 594
- 1 **show boot** on page 597
- 1 **show config** on page 600

md5

Calculates the MD5 checksum for a file in the UNIVERGE WL Controllers nonvolatile storage.

Syntax **md5** [**boot0:** | **boot1:**]*filename*

boot0: | **boot1:** Boot partition into which you copied the file.

filename Name of the file.

Defaults None.

Access Enabled.

Usage You must include the boot partition name in front of the filename. If you specify only the filename, the CLI displays a message stating that the file does not exist.

Examples The following command calculates the checksum for image file UV04240.021 in boot partition 0:

```
pubs# md5 boot0:SR060200.003
MD5 (boot0::SR060200.003) = b9cf7f527f74608e50c70e8fb896392a
```

See Also

- 1 **copy** on page 581
- 1 **dir** on page 584

mkdir

Creates a new subdirectory in nonvolatile storage.

mkdir

Chapter 20

Syntax **mkdir** [*subdirname*]

subdirname Subdirectory name. Specify between 1 and 32 alphanumeric characters, with no spaces.

Defaults None.

Access Enabled.

Examples The following commands create a subdirectory called *corp2* and display the root directory to verify the result:

```
PROMPT# mkdir corp2
success: change accepted.

PROMPT# dir
=====
file:
Filename                               Size             Created
file:configuration                     13 KB            Dec 28 2006, 09:55:54
corp2/                                 1024 bytes       Feb 08 2007, 17:00:51
file:qs_template.xml                   13 KB            Feb 08 2007, 16:33:33
Total:                                27 Kbytes used, 84515 Kbytes free
=====
Boot:
Filename                               Size             Created
boot0:SR060200.002                     8092 KB          Jan 23 2007, 15:51:02
*boot1:SR060200.003                     8103 KB          Feb 05 2007, 19:35:47
Boot0: Total:                          8092 Kbytes used, 9166 Kbytes free
Boot1: Total:                          8103 Kbytes used, 9156 Kbytes free
=====
temporary files:
Filename                               Size             Created
core:command_audit.cur                  159 KB           Feb 08 2007, 16:33:33
core:command_audit.pre                   500 KB           Mar 03 1988, 23:52:03
Total:                                659 Kbytes used, 83908 Kbytes free
```

See Also

- 1 **dir** on page 584
- 1 **rmdir** on page 594

reset system

Restarts a UNIVERGE WL Controller and reboots the software.

Syntax `reset system [force]`

force Immediately restarts the system and reboots, without comparing the running configuration to the configuration file.

Defaults None.

Access Enabled.

Usage If you do not use the **force** option, the command first compares the running configuration to the configuration file. If the running configuration and configuration file do not match, UNIVERGE WL Control System does not restart the UNIVERGE WL Controller but instead displays a message advising you to either save the configuration changes or use the **force** option.

Examples The following command restarts a UNIVERGE WL Controller that does not have any unsaved configuration changes:

```
PROMPT# reset system
This will reset the entire system. Are you sure (y/n)y
```

The following commands attempt to restart a UNIVERGE WL Controller with a running configuration that has unsaved changes, and then force the UNIVERGE WL Controller to restart:

```
PROMPT# reset system
error: Cannot reset, due to unsaved configuration changes. Use "reset system
force" to override.
PROMPT# reset system force
```

See Also

- 1 **save config** on page 594
- 1 **show boot** on page 597
- 1 **show version** on page 602

restore

Unzips a system archive created by the **backup** command and copies the files from the archive onto the UNIVERGE WL Controller.

Syntax **restore system** [**tftp://ip-addr/***filename* [**all** | **critical**] [**force**]

[tftp://ip-addr/] <i>filename</i>	Name of the archive file to load. The archive can be located in the UNIVERGE WL Controllers nonvolatile storage or on a TFTP server.
all	Restores system files <i>and</i> the user files from the archive.
critical	Restores system files only, including the configuration file used when booting, and certificate files.
force	Replaces files on the UNIVERGE WL Controller with those in the archive, even if the UNIVERGE WL Controller is not the same as the one from which the archive was created. CAUTION! Do not use this option unless advised to do so by UNIVERGE. If you restore one UNIVERGE WL Controllers system files onto another UNIVERGE WL Controller, you must generate new key pairs and certificates on the UNIVERGE WL Controller.

Defaults The default is **critical**.

Access Enabled.

Usage If a file in the archive has a counterpart on the UNIVERGE WL Controller, the archive version of the file replaces the file on the UNIVERGE WL Controller. The **restore** command does not delete files that do not have counterparts in the archive. For example, the command does not completely replace the user files area. Instead, files in the archive are added to the user files area. A file in the user area is replaced only if the archive contains a file with the same name.



Note. If the archive's files cannot fit on the UNIVERGE WL Controller, the restore operation fails. UNIVERGE WL Control System recommends deleting unneeded image files before creating or restoring an archive.

The **backup** command stores the MAC address of the UNIVERGE WL Controller in the archive. By default, the **restore** command works only if the MAC address in the archive matches the MAC address of the UNIVERGE WL Controller where the **restore** command is entered. The **force** option overrides this restriction and allows you to unpack one UNIVERGE WL Controllers archive onto another UNIVERGE WL Controller.



Caution! Do not use the **force** option unless you are certain you want to replace the UNIVERGE WL Controllers files with files from another UNIVERGE WL Controller. If you restore one UNIVERGE WL Controlles system files onto another UNIVERGE WL Controller, you must generate new key pairs and certificates on the UNIVERGE WL Controller.

If the configuration running on the UNIVERGE WL Controller is different from the one in the archive or you renamed the configuration file, and you want to retain changes that were made after the archive was created, see the “Managing System Files” chapter of the [Configuration Guide](#).

Examples The following command restores system-critical files on a UNIVERGE WL Controller, from archive *sysa_bak*:

```
PROMPT# restore system tftp://10.10.20.9/sysa_bak
success: received 11908 bytes in 0.150 seconds [ 79386 bytes/sec]
```

```
success: restore complete.
```

See Also **backup** on page 578

rmdir

Removes a subdirectory from nonvolatile storage.

Syntax **rmdir** [*subdirname*]

subdirname Subdirectory name. Specify between 1 and 32 alphanumeric characters, with no spaces.

Defaults None.

Access Enabled.

Usage UNIVERGE WL Control System does not allow the subdirectory to be removed unless it is empty. Delete all files from the subdirectory before attempting to remove it.

Examples The following example removes subdirectory *corp2*:

```
PROMPT# rmdir corp2
success: change accepted.
```

See Also

1 **dir** on page 584

1 **mkdir** on page 589

save config

Saves the running configuration to a configuration file.

Syntax **save config** [*filename*]

filename Name of the configuration file. Specify between 1 and 128 alphanumeric characters, with no spaces.
To save the file in a subdirectory, specify the subdirectory name, followed by a forward slash, in front of the filename.
For example: **backup_configs/config_c**.

Defaults By default, UNIVERGE WL Control System saves the running configuration as the configuration filename used during the last reboot.

Access Enabled.

Usage If you do not specify a filename, UNIVERGE WL Control System replaces the configuration file loaded during the most recent reboot. To display the filename of the configuration file UNIVERGE WL Control System loaded during the most recent reboot, use the **show boot** command.

The command completely replaces the specified configuration file with the running configuration.

Examples The following command saves the running configuration to the configuration file loaded during the most recent reboot. In this example, the filename used during the most recent reboot is *configuration*.

```
PROMPT# save config
success: configuration saved to configuration.
```

The following command saves the running configuration to a file named *testconfig1*:

```
PROMPT# save config testconfig1
success: configuration saved to testconfig1.
```

See Also

- 1 **load config** on page 587
- 1 **show boot** on page 597
- 1 **show config** on page 600

set boot backup-configuration

Specifies the name of a backup configuration file to be used in the event that UNIVERGE WL Control System cannot read the UNIVERGE WL Controllers configuration file at boot time.

set boot configuration-file

Chapter 20

Syntax **set boot backup-configuration** *filename*

filename Name of the file to use as a backup configuration file if UNIVERGE WL Control System cannot read the UNIVERGE WL Controllers configuration file.

Defaults By default, there is no backup configuration file.

Access Enabled.

Examples The following command specifies a file called backup.cfg as the backup configuration file on the UNIVERGE WL Controller:

```
PROMPT# set boot backup-configuration backup.cfg
success: backup boot config filename set.
```

See Also

1 **clear boot backup-configuration** on page 579

1 **show boot** on page 597

set boot configuration-file

Changes the configuration file to load after rebooting.

Syntax **set boot configuration-file** *filename*

filename Filename. Specify between 1 and 128 alphanumeric characters, with no spaces.
To load the file from a subdirectory, specify the subdirectory name, followed by a forward slash, in front of the filename. For example: **backup_configs/config_c**.

Defaults The default configuration filename is *configuration*.

Access Enabled.

Usage The file must be located in the UNIVERGE WL Controllers nonvolatile storage.

Examples The following command sets the boot configuration file to *testconfig1*:

```
PROMPT# set boot configuration-file testconfig1
success: boot config set.
```

set boot partition

Specifies the boot partition in which to look for the system image file following the next system reset, software reload, or power cycle.

Syntax `set boot partition {boot0 | boot1}`

boot0 Boot partition 0.

boot1 Boot partition 1.

Defaults By default, a UNIVERGE WL Controller uses the same boot partition for the next software reload that was used to boot the currently running image.

Access Enabled.

Usage To determine the boot partition that was used to load the currently running software image, use the **dir** command.

Examples The following command sets the boot partition for the next software reload to partition 1:

```
PROMPT# set boot partition boot1
success: Boot partition set to boot1:SR060200.003 (6.0.2.0.003).
```

See Also

- 1 **copy** on page 581
- 1 **dir** on page 584
- 1 **reset system** on page 591

show boot

Displays the system image and configuration filenames used after the last reboot and configured for use after the next reboot.

Syntax `show boot`**Defaults** None.**Access** Access.**Examples** The following command shows the boot information for a UNIVERGE WL Controller:

```
PROMPT# show boot
Configured boot version:      6.0.2.0.003
Configured boot image:       boot0:SC060200.003
Configured boot configuration: file:configuration
Backup boot configuration:    file:backup.cfg
Booted version:              6.0.2.0.003
Booted image:                boot0:SC060200.003
Booted configuration:         file:configuration
Product model:               SCA-WL10
```

Table 76 describes the fields in the **show boot** output.**Table 76. Output for show boot**

Field	Description
Configured boot version	Software version the UNIVERGE WL Controller will run next time the software is rebooted.
Configured boot image	Boot partition and image filename UNIVERGE WL Control System will use to boot next time the software is rebooted.
Configured boot configuration	Configuration filename UNIVERGE WL Control System will use to boot next time the software is rebooted.
Backup boot configuration	The name of the configuration file to be used in the event that UNIVERGE WL Control System cannot read the configured boot configuration file next time the software is rebooted.
Booted version	Software version the UNIVERGE WL Controller is running.

Table 76. Output for show boot

Field	Description
Booted image	Boot partition and image filename UNIVERGE WL Control System used the last time the software was rebooted. UNIVERGE WL Control System is running this software image.
Booted configuration	Configuration filename UNIVERGE WL Control System used to load the configuration the last time the software was rebooted.

See Also

- 1 **clear boot config** on page 580
- 1 **reset system** on page 591
- 1 **set boot configuration-file** on page 596
- 1 **show version** on page 602

show config

Displays the configuration running on the UNIVERGE WL Controller.

Syntax **show config** [**area** *area*] [**all**]

area *area*

Configuration area. You can specify one of the following:

- **aaa**
- **acls**
- **ap**
- **arp**
- **eapol**
- **httpd**
- **ip**
- **ip-config**
- **l2acl**
- **load-balancing**
- **log**
- **mobility-domain**
- **network-domain**
- **ntp**
- **port-group**
- **port config**
- **qos**
- **radio-profile**
- **rfdetect**
- **service-profile**
- **sm**
- **snmp**
- **snoop**
- **spantree**
- **system**
- **trace**
- **vlan**
- **vlan-fdb**
- **vlan-profile**

If you do not specify a configuration area, nondefault information for all areas is displayed.

all

Includes configuration items that are set to their default values.

show version

Chapter 20

Defaults None.

Access Enabled.

Usage If you do not use one of the optional parameters, configuration commands that set nondefault values are displayed for all configuration areas. If you specify an area, commands are displayed for that area only. If you use the **all** option, the display also includes commands for configuration items that are set to their default values.

Examples The following command shows configuration information for VLANs:

```
PROMPT# show config area vlan
# Configuration nvgen'd at 2007-2-08 19:10:33
# Image 6.0.2.0.003
# Model SCA-WL10
# Last change occurred at 2007-2-08 19:02:15
set vlan 1 port 1
```

See Also

1 **load config** on page 587

1 **save config** on page 594

show version

Displays software and hardware version information for a UNIVERGE WL Controller and, optionally, for any attached UNIVERGE WL Access Points.

Syntax **show version** [**details**]

details Includes additional software build information and information about the UNIVERGE WL Access Points configured on the UNIVERGE WL Controller.

Defaults None

Access All.

Examples The following command displays version information for a UNIVERGE WL Controller:

PROMPT# show version

```
UNIVERGE WL System Software V1, Version: 6.0.3.0 REL
Copyright (c) 2006 - 2007 NEC Infrontia Corporation. All rights reserved.
```

```
Build Information: 0.1 011 2007-04-16 16:32:00
Model:             WL1700-MS
Hardware
  Mainboard:       version 1 ; revision 1
Serial number      0909090909
Flash:             1.0.0.0 - FROM0
Kernel:            2.6.10_mvl401-SV011
BootLoader:        6.0.13 / 6.0.13
```

The following command displays additional software build information and AP access point information:

PROMPT# show version details

```
UNIVERGE WL System Software V1, Version: 6.0.3.0 REL
Copyright (c) 2006 - 2007 NEC Infrontia Corporation. All rights reserved.
```

```
Build Information: 0.1 011 2007-04-16 16:32:00
Label:             REL_6.0.3.0.011_041607
Model:             WL1700-MS
Hardware
  Mainboard:       version 1 ; revision 1
  CPU Model:       440GR
Serial number      0909090909
Flash:             1.0.0.0 - FROM0
Kernel:            2.6.10_mvl401-SV011
BootLoader:        6.0.13 / 6.0.13
```

AP	AP Model	Serial #	Versions
1	WL1700-MS(AP	0909090909	H/W : 1
			F/W1 : N/A
			F/W2 : N/A
			S/W : REL_6.0.3.0.011_041607
			BOOT S/W : REL_6.0.3.0.011_041607
			fingerprint :

Table 77 describes the fields in the **show version** output.

Table 77. Output for show version

Field	Description
Build Information	Factory timestamp of the image file.
Label	Software version and build date.
Build Suffix	Build suffix.
Model	Build model.
Hardware	Version information for the UNIVERGE WL Controllers motherboard and Power over Ethernet (PoE) board.
Serial number	Serial number of the UNIVERGE WL Controller.
Flash	Flash memory version.
Kernel	Kernel version.
BootLoader	Boot code version.
Port/AP	Port number connected to an AP access point.
Serial #	AP serial number.
Versions	AP hardware, firmware, and software versions.

See Also **show boot** on page 597

Trace Commands

Use trace commands to perform diagnostic routines. While UNIVERGE WL Control System allows you to run many types of traces, this chapter describes commands for those traces you are most likely to use. For a complete listing of the types of traces UNIVERGE WL Control System allows, type the **set trace ?** command.



Caution! Using the **set trace** command can have adverse effects on system performance. UNIVERGE WL Control System recommends that you use the lowest levels possible for initial trace commands, and slowly increase the levels to get the data you need.

This chapter presents trace commands alphabetically. Use the following table to locate commands in this chapter based on their use.

Trace	set trace sm on page 611
	set trace dot1x on page 610
	set trace authentication on page 607
	set trace authorization on page 608
	show trace on page 611
	save trace on page 607
	clear log trace on page 606

clear log trace

Deletes the log messages stored in the trace buffer.

Syntax `clear log trace`

Defaults None.

Access Enabled.

Examples To delete the trace log, type the following command:

```
PROMPT# clear log trace
```

See Also

1 **set log** on page 626

1 **show log buffer** on page 630

clear trace

Deletes running trace commands and ends trace processes.

Syntax `clear trace {trace-area | all}`

trace-area Ends a particular trace process. Specify one of the following keywords to end the traces documented in this chapter:

- **authorization**—Ends an authorization trace
- **dot1x**—Ends an 802.1X trace
- **authentication**—Ends an authentication trace
- **sm**—Ends a session manager trace

all Ends all trace processes.

Defaults None.

Access Enabled.

Examples To clear all trace processes, type the following command:

```
PROMPT# clear trace all
success: clear trace all
```

To clear the session manager trace, type the following command:

```
PROMPT# clear trace sm  
success: clear trace sm
```

See Also

- 1 **set trace authentication** on page 607
- 1 **set trace authorization** on page 608
- 1 **set trace dot1x** on page 610
- 1 **set trace sm** on page 611
- 1 **show trace** on page 611

save trace

Saves the accumulated trace data for enabled traces to a file in the UNIVERGE WL Controller's nonvolatile storage.

Syntax `save trace filename`

filename Name for the trace file. To save the file in a subdirectory, specify the subdirectory name, then a slash. For example: **traces/trace1**

Defaults None.

Access Enabled.

Examples To save trace data into the file *trace1* in the subdirectory *traces*, type the following command:

```
PROMPT# save trace traces/trace1
```

set trace authentication

Traces authentication information.

set trace authorization

Chapter 21

Syntax **set trace authentication** [**mac-addr** *mac-address*] [**port** *port-num*]
[**user** *username*] [**level** *level*]

mac-addr <i>mac-address</i>	Traces a MAC address. Specify a MAC address, using colons to separate the octets (for example, 00:11:22:aa:bb:cc).
port <i>port-num</i>	Traces a port number.
user <i>username</i>	Traces a user. Specify a username of up to 32 alphanumeric characters with no spaces.
level <i>level</i>	Determines the quantity of information included in the output. You can set the level with an integer from 1 to 10, where level 10 provides the most information. Levels 1 through 5 provide user-readable information. If you do not specify a level, level 5 is the default.

Defaults The default trace level is 5.

Access Enabled.

Examples The following command starts a trace for information about user *jose*'s authentication:

```
PROMPT# set trace authentication user jose
success: change accepted.
```

See Also

1 **clear trace** on page 606

1 **show trace** on page 611

set trace authorization

Traces authorization information.

Syntax **set trace authorization** [**mac-addr** *mac-address*] [**port** *port-num*] [**user** *username*] [**level** *level*]

mac-addr <i>mac-address</i>	Traces a MAC address. Specify a MAC address, using colons to separate the octets (for example, 00:11:22:aa:bb:cc).
port <i>port-num</i>	Traces a port number.
user <i>username</i>	Traces a user. Specify a username of up to 80 alphanumeric characters with no spaces.
level <i>level</i>	Determines the quantity of information included in the output. You can set the level with an integer from 1 to 10, where level 10 provides the most information. Levels 1 through 5 provide user-readable information. If you do not specify a level, level 5 is the default.

Defaults The default trace level is 5.

Access Enabled.

Examples The following command starts a trace for information for authorization for MAC address 00:01:02:03:04:05

```
PROMPT# set trace authorization mac-addr 00:01:02:03:04:05
success: change accepted.
```

See Also

1 **clear trace** on page 606

1 **show trace** on page 611

set trace dot1x

Traces 802.1X sessions.

Syntax **set trace dot1x** [**mac-addr** *mac-address*] [**port** *port-num*] [**user** *username*] [**level** *level*]

mac-addr <i>mac-address</i>	Traces a MAC address. Specify a MAC address, using colons to separate the octets (for example, 00:11:22:aa:bb:cc).
port <i>port-num</i>	Traces a port number.
user <i>username</i>	Traces a user. Specify a username of up to 80 alphanumeric characters with no spaces.
level <i>level</i>	Determines the quantity of information included in the output. You can set the level with an integer from 1 to 10, where level 10 provides the most information. Levels 1 through 5 provide user-readable information. If you do not specify a level, level 5 is the default.

Defaults The default trace level is 5.

Access Enabled.

Examples The following command starts a trace for the 802.1X sessions for MAC address 00:01:02:03:04:05

```
PROMPT# set trace dot1x mac-addr 00:01:02:03:04:05
success: change accepted.
```

See Also

- 1 **clear trace** on page 606
- 1 **show trace** on page 611

set trace sm

Traces session manager activity.

Syntax **set trace sm** [**mac-addr** *mac-address*] [**port** *port-num*] [**user** *username*] [**level** *level*]

mac-addr <i>mac-address</i>	Traces a MAC address. Specify a MAC address, using colons to separate the octets (for example, 00:11:22:aa:bb:cc).
port <i>port-num</i>	Traces a port number.
user <i>username</i>	Traces a user. Specify a username of up to 80 alphanumeric characters, with no spaces.
level <i>level</i>	Determines the quantity of information included in the output. You can set the level with an integer from 1 to 10, where level 10 provides the most information. Levels 1 through 5 provide user-readable information. If you do not specify a level, level 5 is the default.

Defaults The default trace level is 5.

Access Enabled.

Examples Type the following command to trace session manager activity for MAC address 00:01:02:03:04:05

```
PROMPT# set trace sm mac-addr 00:01:02:03:04:05
success: change accepted.
```

See Also

- 1 **clear trace** on page 606
- 1 **show trace** on page 611

show trace

Displays information about traces that are currently configured on the UNIVERGE WL Controller, or all possible trace options.

show trace

Chapter 21

Syntax **show trace** [**all**]

all Displays all possible trace options and their configuration.

Defaults None.

Access Enabled.

Examples To view the traces currently running, type the following command:

PROMPT# **show trace**

Trace Area	Level	Mac	User	Port	Filter
-----	-----	-----	-----	-----	-----
dot1x	5				0
sm	5				0

See Also

- 1 **clear trace** on page 606
- 1 **set trace authentication** on page 607
- 1 **set trace authorization** on page 608
- 1 **set trace dot1x** on page 610
- 1 **set trace sm** on page 611

Snoop Commands

Use snoop commands to monitor wireless traffic, by using a UNIVERGE WL Access Point as a sniffing device. The UNIVERGE WL Access Points copies the sniffed 802.11 packets and sends the copies to an observer, typically a protocol analyzer such as Ethereal or Tethereal.

(For more information, including setup instructions for the monitoring station, see the “Remotely Monitoring Traffic” section in the “Troubleshooting a UNIVERGE WL Controller chapter of the [Configuration Guide](#).)

This chapter presents snoop commands alphabetically. Use the following table to locate commands in this chapter based on their use.

Remote monitoring (snooping)	set snoop on page 616
	show snoop info on page 621
	clear snoop on page 614
	set snoop map on page 618
	show snoop map on page 621
	show snoop on page 620
	clear snoop map on page 614
	set snoop mode on page 619
	show snoop stats on page 622

clear snoop

Deletes a snoop filter.

Syntax `clear snoop filter-name`

filter-name Name of the snoop filter.

Defaults None.

Access Enabled.

Examples The following command deletes snoop filter *snoop1*:

```
PROPMT# clear snoop snoop1
```

See Also

1 **set snoop** on page 616

1 **show snoop info** on page 621

clear snoop map

Removes a snoop filter from a UNIVERGE WL Access Point radio.

Examples `clear snoop map filter-name ap ap-num radio {1 | 2}`

filter-name Name of the snoop filter.

ap *ap-num* Number of a UNIVERGE WL Access Points to which to snoop filter is mapped.

radio 1 Radio 1 of the UNIVERGE WL Access Points.

radio 2 Radio 2 of the UNIVERGE WL Access Points. (This option does not apply to single-radio models.)

Defaults None.

Access Enabled.

Examples The following command removes snoop filter *snoop2* from radio 2 on UNIVERGE WL Access Points 3:

```
PROPMT# clear snoop map snoop2 ap 3 radio 2
success: change accepted.
```

The following command removes all snoop filter mappings from all radios:

```
PROPMT# clear snoop map all
success: change accepted.
```

See Also

- 1 **set snoop map** on page 618
- 1 **show snoop** on page 620
- 1 **show snoop map** on page 621

set snoop

Configures a snoop filter.

Syntax `set snoop filter-name [condition-list] [observer ip-addr] [snap-length num]`

filter-name Name for the filter. The name can be up to 15 alphanumeric characters, with no spaces.

condition-list Match criteria for packets. Conditions in the list are ANDed. Therefore, to be copied and sent to an observer, a packet must match all criteria in the *condition-list*. You can specify up to eight of the following conditions in a filter, in any order or combination:

- **frame-type** {eq | neq} {beacon | control | data | management | probe}
- **channel** {eq | neq} *channel*
- **bssid** {eq | neq} *bssid*
- **src-mac** {eq | neq | lt | gt} *mac-addr*
- **dest-mac** {eq | neq | lt | gt} *mac-addr*
- **host-mac** {eq | neq | lt | gt} *mac-addr*
- **mac-pair** *mac-addr1 mac-addr2*
- **direction** {eq | neq} {transmit | receive}

To match on packets to or from a specific MAC address, use the **dest-mac** or **src-mac** option. To match on both send and receive traffic for a host address, use the **host-mac** option. To match on a traffic flow (source and destination MAC addresses), use the **mac-pair** option. This option matches for either direction of a flow, and either MAC address can be the source or destination address.

If you omit a condition, all packets match that condition. For example, if you omit **frame-type**, all frame types match the filter.

For most conditions, you can use **eq** (equal) to match only on traffic that matches the condition value. Use **neq** (not equal) to match only on traffic that is not equal to the condition value.

The **src-mac**, **dest-mac**, and **host-mac** conditions also support **lt** (less than) and **gt** (greater than).

- observer** *ip-addr* Specifies the IP address of the station where the protocol analyzer is located. If you do not specify an observer, the UNIVERGE WL Access Points radio still counts the packets that match the filter.
- snap-length** *num* Specifies the maximum number of bytes to capture. If you do not specify a length, the entire packet is copied and sent to the observer. UNIVERGE WL Control System recommends specifying a snap length of 100 bytes or less.

Defaults No snoop filters are configured by default.

Access Enabled.

Usage Traffic that matches a snoop filter is copied after it is decrypted. The decrypted (clear) version is sent to the observer.

For best results:

- 1 Do not specify an observer that is associated with the UNIVERGE WL Access Points where the snoop filter is running. This configuration causes an endless cycle of snoop traffic.
- 1 If the snoop filter is running on a UNIVERGE WL Access Points, and the UNIVERGE WL Access Points used a DHCP server in its local subnet to configure its IP information, and the UNIVERGE WL Access Points did not receive a default router (gateway) address as a result, the observer must also be in the same subnet. Without a default router, the UNIVERGE WL Access Points cannot find the observer.
- 1 The UNIVERGE WL Access Points that is running a snoop filter forwards snooped packets directly to the observer. This is a one-way communication, from the UNIVERGE WL Access Points to the observer. If the observer is not present, the UNIVERGE WL Access Points still sends the snoop packets, which use bandwidth. If the observer is present but is not listening to TZSP traffic, the observer continuously sends ICMP error indications back to the UNIVERGE WL Access Points. These ICMP messages can affect network and UNIVERGE WL Access Points performance.

Examples The following command configures a snoop filter named *snoop1* that matches on all traffic, and copies the traffic to the device that has IP address 10.10.30.2:

```
PROPMT# set snoop snoop1 observer 10.10.30.2 snap-length 100
```

set snoop map

Chapter 22

The following command configures a snoop filter named *snoop2* that matches on all data traffic between the device with MAC address aa:bb:cc:dd:ee:ff and the device with MAC address 11:22:33:44:55:66, and copies the traffic to the device that has IP address 10.10.30.3:

```
PROPMT# set snoop snoop2 frame-type eq data mac-pair aa:bb:cc:dd:ee:ff
11:22:33:44:55:66 observer 10.10.30.3 snap-length 100
```

See Also

- 1 **clear snoop** on page 614
- 1 **set snoop map** on page 618
- 1 **set snoop mode** on page 619
- 1 **show snoop info** on page 621
- 1 **show snoop stats** on page 622

set snoop map

Maps a snoop filter to a radio on a UNIVERGE WL Access Points. A snoop filter does take effect until you map it to a radio and enable the filter.

Examples `set snoop map filter-name ap ap-num radio {1 | 2}`

<i>filter-name</i>	Name of the snoop filter.
ap <i>ap-num</i>	Number of a UNIVERGE WL Access Points to which to map the snoop filter.
radio 1	Radio 1 of the UNIVERGE WL Access Points.
radio 2	Radio 2 of the UNIVERGE WL Access Points. (This option does not apply to single-radio models.)

Defaults Snoop filters are unmapped by default.

Access Enabled.

Usage You can map the same filter to more than one radio. You can map up to eight filters to the same radio. If more than one filter has the same observer, the UNIVERGE WL Access Points sends only one copy of a packet that matches a filter to the observer. After the first match, the UNIVERGE WL Access Points sends the packet and stops comparing the packet against other filters for the same observer.

If the filter does not have an observer, the UNIVERGE WL Access Points still maintains a counter of the number of packets that match the filter. (See **show snoop stats** on page 622.)

Examples The following command maps snoop filter *snoop1* to radio 2 on UNIVERGE WL Access Points 3:

```
PROPMT# set snoop map snoop1 ap 3 radio 2
success: change accepted.
```

See Also

- 1 **clear snoop map** on page 614
- 1 **set snoop** on page 616
- 1 **set snoop mode** on page 619
- 1 **show snoop map** on page 621
- 1 **show snoop stats** on page 622

set snoop mode

Enables a snoop filter. A snoop filter does not take effect until you map it to a UNIVERGE WL Access Point radio and enable the filter.

Examples **set snoop** *{filter-name | all}* **mode** {enable | disable}

<i>filter-name</i> all	Name of the snoop filter. Specify all to enable all snoop filters.
enable	Enables the snoop filter.
disable	Disables the snoop filter.

Defaults Snoop filters are disabled by default.

show snoop

Chapter 22

Access Enabled.

Usage The filter mode is retained even if you disable and reenable the radio, or restart the UNIVERGE WL Access Points or the UNIVERGE WL Controller. Once the filter is enabled, you must use the disable option to disable it.

Examples The following command enables snoop filter *snoop1*:

```
PROPMT# set snoop snoop1 mode enable
success: filter 'snoop1' enabled
```

See Also

- 1 **show snoop** on page 620
- 1 **show snoop info** on page 621
- 1 **show snoop map** on page 621
- 1 **show snoop stats** on page 622

show snoop

Displays the UNIVERGE WL Access Points radio mapping for all snoop filters.

Syntax **show snoop**

Defaults None.

Access Enabled.

Usage To display the mappings for a specific UNIVERGE WL Access Points radio, use the **show snoop map** command.

Examples The following command shows the UNIVERGE WL Access Points radio mappings for all snoop filters configured on a UNIVERGE WL Controller:

```
PROPMT# show snoop
AP: 3      Radio: 2
           snoop1
           snoop2
AP: 2      Radio: 2
           snoop2
```

See Also

- 1 **clear snoop map** on page 614

- 1 **set snoop map** on page 618
- 1 **show snoop map** on page 621

show snoop info

Shows the configured snoop filters.

Syntax **show snoop** *filter-name*

filter-name Name of the snoop filter.

Defaults None.

Access Enabled.

Examples The following command shows the snoop filters configured in the examples above:

```
PROPMT# show snoop info
snoop1:
  observer 10.10.30.2 snap-length 100
  all packets
snoop2:
  observer 10.10.30.3 snap-length 100
  frame-type eq data
  mac-pair (aa:bb:cc:dd:ee:ff, 11:22:33:44:55:66)
```

See Also

- 1 **clear snoop** on page 614
- 1 **set snoop** on page 616

show snoop map

Shows the UNIVERGE WL Access Points radios that are mapped to a specific snoop filter.

Syntax **show snoop map** *filter-name*

filter-name Name of the snoop filter.

show snoop stats

Chapter 22

Defaults None.

Access Enabled.

Usage To display the mappings for all snoop filters, use the **show snoop** command.

Examples The following command shows the mapping for snoop filter *snoop1*:

```
PROPMT# show snoop map snoop1
filter 'snoop1' mapping
      AP: 3      Radio: 2
```

See Also

1 **clear snoop map** on page 614

1 **set snoop map** on page 618

1 **show snoop** on page 620

show snoop stats

Displays statistics for enabled snoop filters.

Examples **show snoop stats** [*filter-name* **ap** [*ap-num* [**radio** {**1** | **2**}]]]

filter-name Name of the snoop filter.

ap *ap-num* Number of a UNIVERGE WL Access Points to which the snoop filter is mapped.

radio 1 Radio 1 of the UNIVERGE WL Access Points.

radio 2 Radio 2 of the UNIVERGE WL Access Points. (This option does not apply to single-radio models.)

Defaults None.

Access Enabled.

Usage The UNIVERGE WL Access Points retains statistics for a snoop filter until the filter is changed or disabled. The UNIVERGE WL Access Points then clears the statistics.

Examples The following command shows statistics for snoop filter *snoop1*:

```

PROPMT# show snoop stats snoop1
Filter      AP  Radio  Rx Match  Tx Match  Dropped
=====
snoop1      3    1      96        4         0

```

Table 78 describes the fields in this display.

Table 78. show snoop stats Output

Field	Description
Filter	Name of the snoop filter.
AP	UNIVERGE WL Access Points containing the radio to which the filter is mapped.
Radio	Radio to which the filter is mapped.
Rx Match	Number of packets received by the radio that match the filter.
Tx Match	Number of packets sent by the radio that match the filter.
Dropped	Number of packets that matched the filter but that were not copied to the observer due to memory or network problems.

show snoop stats

Chapter 22

System Log Commands

Use the system log commands to record information for monitoring and troubleshooting. UNIVERGE WL Control System system logs are based on RFC 3164, which defines the log protocol.

This chapter presents system log commands alphabetically. Use the following table to locate commands in this chapter based on their use.

System Logs	set log on page 626
	set log mark on page 629
	show log buffer on page 630
	show log trace on page 633
	clear log on page 625

clear log

Clears the log messages stored in the log buffer, or removes the configuration for a syslog server and stops sending log messages to that server.

Syntax **clear log** [**buffer** | **server** *ip-addr*]

buffer	Deletes the log messages stored in nonvolatile storage.
server <i>ip-addr</i>	Deletes the configuration for and stops sending log messages to the syslog server at this IP address. Specify an address in dotted decimal notation.

Defaults None.

Access Enabled.

Examples To stop sending system logging messages to a server at 192.168.253.11, type the following command:

```
PROPMT# clear log server 192.168.253.11
success: change accepted.
```

Type the following command to clear all messages from the log buffer:

```
PROPMT# clear log buffer
success: change accepted.
```

See Also

- 1 **clear log trace** on page 606
- 1 **set log** on page 626

set log

Enables or disables logging of UNIVERGE WL Controller and AP events to the UNIVERGE WL Controller log buffer or other logging destination and sets the level of the events logged. For logging to a syslog server only, you can also set the facility logged.

Syntax **set log** { **buffer** | **console** | **current** | **sessions** | **trace** }
[**severity** *severity-level*] [**enable** | **disable**]

set log server *ip-addr* [**port** *port-number*] **severity** *severity-level*
[**local-facility** *facility-level*]

buffer	Sets log parameters for the log buffer in nonvolatile storage.
console	Sets log parameters for console sessions.
current	Sets log parameters for the current Telnet or console session. These settings are not stored in nonvolatile memory.
server <i>ip-addr</i>	Sets log parameters for a syslog server. Specify an address in dotted decimal notation.

sessions	<p>Sets the default log values for Telnet sessions. You can set defaults for the following log parameters:</p> <ul style="list-style-type: none">• Severity• Logging state (enabled or disabled) <p>To override the session defaults for an individual session, type the set log command from within the session and use the current option.</p>
trace	<p>Sets log parameters for trace files.</p>
port <i>port-number</i>	<p>Sets the TCP port for sending messages to the syslog server. You can specify a number from 1 to 65535. The default syslog port is 514.</p>
severity <i>severity-level</i>	<p>Logs events at a severity level greater than or equal to the level specified. Specify one of the following:</p> <ul style="list-style-type: none">• emergency—The UNIVERGE WL Controller is unusable.• alert—Action must be taken immediately.• critical—You must resolve the critical conditions. If the conditions are not resolved, the UNIVERGE WL Controller can reboot or shut down.• error—The UNIVERGE WL Controller is missing data or is unable to form a connection.• warning—A possible problem exists.• notice—Events that potentially can cause system problems have occurred. These are logged for diagnostic purposes. No action is required.• info—Informational messages only. No problem exists.• debug—Output from debugging.

local-facility
facility-level

For messages sent to a syslog server, maps all messages of the severity you specify to one of the standard local log facilities defined in RFC 3164. You can specify one of the following values:

- **0**—maps all messages to *local0*.
- **1**—maps all messages to *local1*.
- **2**—maps all messages to *local2*.
- **3**—maps all messages to *local3*.
- **4**—maps all messages to *local4*.
- **5**—maps all messages to *local5*.
- **6**—maps all messages to *local6*.
- **7**—maps all messages to *local7*.

If you do not specify a local facility, UNIVERGE WL Control System sends the messages with their default UNIVERGE WL Control System facilities. For example, AAA messages are sent with facility 4 and boot messages are sent with facility 20 by default.

enable

Enables messages to the specified target.

disable

Disables messages to the specified target.

Defaults

- 1 Events at the error level and higher are logged to the UNIVERGE WL Controller console.
- 1 Events at the error level and higher are logged to the UNIVERGE WL Controller system buffer.
- 1 Trace logging is enabled, and debug-level output is stored in the UNIVERGE WL Controller trace buffer.

Access Enabled.

Usage Using the command with only **enable** or **disable** turns logging on or off for the target at all levels. For example, entering **set log buffer enable** with no other keywords turns on logging to the system buffer of all facilities at all levels. Entering **set log buffer disable** with no other keywords turns off all logging to the buffer.

Examples To log only emergency, alert, and critical system events to the console, type the following command:

```
PROPMT# set log console severity critical enable
success: change accepted.
```

See Also

1 **show log config** on page 632

1 **clear log** on page 625

set log mark

Configures UNIVERGE WL Control System to generate mark messages at regular intervals. The mark messages indicate the current system time and date. NEC Networks can use the mark messages to determine the approximate time when a system restart or other event causing a system outage occurred.

Syntax **set log mark** [**enable** | **disable**] [**severity** *level*]
[**interval** *interval*]

enable Enables the mark messages.

disable Disables the mark messages.

severity *level* Log severity at which the messages are logged:

- **emergency**
- **alert**
- **critical**
- **error**
- **warning**
- **notice**
- **info**
- **debug**

interval *interval* Interval at which UNIVERGE WL Control System generates the mark messages. You can specify from 1 to 2147483647 seconds.

Defaults Mark messages are disabled by default. When they are enabled, UNIVERGE WL Control System generates a message at the notice level once every 300 seconds by default.

Access Enabled.

Examples The following command enables mark messages:

```
PROPMT# set log mark enable
success: change accepted.
```

See Also **show log config** on page 632

show log buffer

Displays system information stored in the nonvolatile log buffer or the trace buffer.

Syntax **show log buffer** [{+|-}*number-of-messages*] [**facility** *facility-name*] [**matching** *string*] [**severity** *severity-level*]

buffer	Displays the log messages in nonvolatile storage.
+ -<i>number-of-messages</i>	Displays the number of messages specified as follows: <ul style="list-style-type: none">• A positive number (for example, +100), displays that number of log entries starting from the oldest in the log.• A negative number (for example, -100) displays that number of log entries starting from newest in the log.
facility <i>facility-name</i>	Area of UNIVERGE WL Control System that is sending the log message. Type a space and a question mark (?) after show log buffer facility for a list of valid facilities.
matching <i>string</i>	Displays messages that match a string—for example, a username or IP address.

- severity** *severity-level* Displays messages at a severity level greater than or equal to the level specified. Specify one of the following:
- **emergency**—The UNIVERGE WL Controller is unusable.
 - **alert**—Action must be taken immediately.
 - **critical**—You must resolve the critical conditions. If the conditions are not resolved, the UNIVERGE WL Controller can reboot or shut down.
 - **error**—The UNIVERGE WL Controller is missing data or is unable to form a connection.
 - **warning**—A possible problem exists.
 - **notice**—Events that potentially can cause system problems have occurred. These are logged for diagnostic purposes. No action is required.
 - **info**—Informational messages only. No problem exists.
 - **debug**—Output from debugging.

Defaults None.

Access Enabled.

Usage The debug level produces a lot of messages, many of which can appear to be somewhat cryptic. Debug messages are used primarily by NEC Networks for troubleshooting and are not intended for administrator use.

Examples Type the following command to see the facilities for which you can view event messages archived in the buffer:

```
PROPMT# show log buffer facility ?
```

```
<facility name>      Select one of: KERNEL, AAA, SYSLOGD, ACL, APM, ARP, ASO,
                     BOOT, CLI, CLUSTER, CRYPTO, DOT1X, NET, ETHERNET, GATEWAY, HTTPD, IGMP, IP,
                     MISC, NOSE, NP, RAND, RESOLV, RIB, ROAM, ROGUE, SM, SNMPD, SPAN, STORE, SYS,
                     TAGMGR, TBRIDGE, TCPSSL, TELNET, TFTP, TLS, TUNNEL, VLAN, X509, XML, MP,
                     RAPDA, WEBVIEW, EAP, FP, STAT, SSHD, SUP, DNSD, CONFIG, BACKUP.
```

The following command displays logged messages for the AAA facility:

```
PROPMT# show log buffer facility AAA
```

```
AAA Jun. 25 09:11:32.579848 ERROR AAA_NOTIFY_ERR: AAA got SM special event (98)
on locality 3950 which is gone
```

See Also

- 1 **clear log** on page 625
- 1 **show log config** on page 632

show log config

Displays log configuration information.

Syntax **show log config**

Defaults None.

Access Enabled.

Examples To display how logging is configured, type the following command:

```
PROPMT# show log config
Logging console:           disabled
Logging console severity:  DEBUG
Logging sessions:         disabled
Logging sessions severity: INFO
Logging buffer:           enabled
Logging buffer severity:   WARNING
Logging trace:            enabled
Logging trace severity:    DEBUG
Logging buffer size:       10485760 bytes
Log marking:              disabled
Log marking severity:      NOTICE
Log marking interval:      300 seconds

Logging server:            172.21.12.19 port 514 severity EMERGENCY

Current session:          disabled
Current session severity:  INFO
```

See Also

- 1 **set log** on page 626
- 1 **clear log** on page 625

show log trace

Displays system information stored in the nonvolatile log buffer or the trace buffer.

Syntax **show log trace** [{+|-|/}*number-of-messages*] [**facility** *facility-name*] [**matching** *string*] [**severity** *severity-level*]

trace	Displays the log messages in the trace buffer.
+ - / <i>number-of-messages</i>	Displays the number of messages specified as follows: <ul style="list-style-type: none">• A positive number (for example, +100), displays that number of log entries starting from the oldest in the log.• A negative number (for example, -100) displays that number of log entries starting from newest in the log.• A number preceded by a slash (for example, /100) displays that number of the most recent log entries in the log, starting with the least recent.
facility <i>facility-name</i>	Area of UNIVERGE WL Control System that is sending the log message. Type a space and a question mark (?) after show log trace facility for a list of valid facilities.

matching <i>string</i>	Displays messages that match a string—for example, a username or IP address.
severity <i>severity-level</i>	<p>Displays messages at a severity level greater than or equal to the level specified. Specify one of the following:</p> <ul style="list-style-type: none">• emergency—The UNIVERGE WL Controller is unusable.• alert—Action must be taken immediately.• critical—You must resolve the critical conditions. If the conditions are not resolved, the UNIVERGE WL Controller can reboot or shut down.• error—The UNIVERGE WL Controller is missing data or is unable to form a connection.• warning—A possible problem exists.• notice—Events that potentially can cause system problems have occurred. These are logged for diagnostic purposes. No action is required.• info—Informational messages only. No problem exists.• debug—Output from debugging.

Defaults None.

Access Enabled.

Examples Type the following command to see the facilities for which you can view event messages archived in the buffer:

```
PROPMT# show log trace facility ?
<facility name> Select one of: KERNEL, AAA, SYSLOGD, ACL, APM, ARP, ASO, BOOT,
CLI, CLUSTER, CRYPTO, DOT1X, ENCAP, ETHERNET, GATEWAY, HTTPD, IGMP, IP, MISC,
NOSE, NP, RAND, RESOLV, RIB, ROAM, ROGUE, SM, SNMPD, SPAN, STORE, SYS, TAGMGR,
TBRIDGE, TCPSSL, TELNET, TFTP, TLS, TUNNEL, VLAN, X509, XML, MP, RAPDA, WEBVIEW,
EAP, PORTCONFIG, FP.
```

The following command displays the newest five trace log entries for the ROGUE facility:

```
PROPMT# show log trace +5 facility ROGUE
ROGUE Oct 28 16:30:19.695141 ERROR ROGUE_AP_ALERT: Xmtr Mac 01:0b:0e:ff:00:3b Ap
7 Radio 1 Chan 36 RSSI 18 Tech DOT_11A SSID univerge
                                ROGUE Oct 28 16:30:19.7046
37 ERROR ROGUE_AP_ALERT: Xmtr Mac 00:60:b9:11:57:co Ap 7 Radio 1 Chan 36 RSSI
15 Tech DOT_11A SSID examplewlan
                                ROGUE Oct 28 16:30:19.711253 ERROR ROGUE_AP_ALER
```

```
T: Xmtr Mac 00:60:b9:11:58:co Ap 7 Radio 1 Chan 36 RSSI 36 Tech DOT_11A SSID
wlan-7
      ROGUE Oct 28 16:30:19.717954 ERROR ROGUE_AP_ALERT: Xmtr Mac 00:0b:0e:00:0
6:8f Ap 7 Radio 1 Chan 36 RSSI 13 Tech DOT_11A SSID univerge
      ROGUE Oct 28 16:30:
19.727069 ERROR ROGUE_AP_ALERT: Xmtr Mac 00:60:b9:11:52:co Ap 7 Radio 1 Chan 3
6 RSSI 22 Tech DOT_11A SSID univerge
```

See Also

- 1 **clear log** on page 625
- 1 **show log config** on page 632

show log trace

Chapter 23

Index

B

backup 578

C

clear accounting 185
clear ap 45
clear ap boot-configuration 273
clear ap radio 271
clear authentication admin 186
clear authentication console 187
clear authentication dot1x 188
clear authentication last-resort 189
clear authentication mac 189
clear authentication web 190
clear banner motd 22
clear boot backup-configuration 579
clear boot config 580
clear dot1x max-req 515
clear dot1x quiet-period 515
clear dot1x reauth-max 516
clear dot1x reauth-period 516
clear dot1x timeout auth-server 517
clear dot1x timeout supplicant 517
clear dot1x tx-period 518
clear fdb 66
clear history 22
clear igmp statistics 428
clear interface 97
clear ip alias 98
clear ip dns domain 99
clear ip dns server 99
clear ip route 100
clear ip telnet 101
clear location policy 190
clear log 625
clear log buffer 625
clear log server 625
clear log trace 606
clear mac-user 191
clear mac-user attr 192
clear mac-user group 193
clear mac-usergroup 193
clear mac-usergroup attr 194
clear mobility-domain 250
clear mobility-domain member 250
clear mobility-profile 195
clear network-domain 258
clear network-domain mode 258
clear network-domain peer 259
clear network-domain seed-ip 260
clear ntp server 102
clear ntp update-interval 102
clear port counters 46
clear port name 47
clear qos 90
clear radio-profile 275
clear radius 500
clear radius client system-ip 501
clear radius server 502
clear rfdetect attack-list 548
clear rfdetect black-list 549
clear rfdetect ignore 549
clear rfdetect ssid-list 550
clear rfdetect vendor-list 550
clear security acl 454
clear security acl map 456
clear security l2-restrict 67
clear security l2-restrict counters 68
clear server group 502
clear server group load-balance 502
clear service-profile 276
clear sessions 531
clear sessions network 532
clear snmp community 103
clear snmp notify profile 103
clear snmp notify target 104
clear snmp usm 105
clear snoop 614
clear snoop map 614
clear summertime 105
clear system 23
clear system countrycode 23
clear system ip-address 23, 106
clear system location 24
clear system name 23
clear timezone 107

- clear trace 606
- clear user 196
- clear user attr 196
- clear user group 197
- clear usergroup 198
- clear usergroup attr 199
- clear vlan 69
- commit security acl 458
- copy 581
- crypto ca-certificate 482
- crypto ca-certificate admin 482
- crypto ca-certificate eap 482
- crypto certificate 483
- crypto certificate admin 483
- crypto certificate eap 483
- crypto generate key 485
- crypto generate request 486
- crypto generate request admin 486
- crypto generate request eap 486
- crypto generate self-signed 489
- crypto generate self-signed admin 489
- crypto generate self-signed eap 489
- crypto otp 491
- crypto otp admin 491
- crypto otp eap 491
- crypto pkcs12 492
- crypto pkcs12 admin 492
- crypto pkcs12 eap 492

D

- delete 583
- dir 584
- disable 17

E

- enable 17

H

- help 25
- history 26

L

- load config 587

M

- md5 589
- mkdir 589
- monitor port counters 47

P

- ping 107

Q

- quit 18

R

- reset ap 277
- reset port 53
- reset system 591
- restore 592
- rfping 551
- rmdir 594
- rollback security acl 459

S

- save config 594
- save trace 607
- set accounting {admin | console} 200
- set accounting {dot1x | mac | web} 201
- set ap 54
- set ap auto 277
- set ap auto mode 279
- set ap auto persistent 280
- set ap auto radiotype 281
- set ap bias 282
- set ap blink 283
- set ap boot-configuration ip 284
- set ap boot-configuration switch 285
- set ap boot-configuration vlan 287
- set ap fingerprint 288
- set ap force-image-download 289
- set ap name 290
- set ap radio antennatype 291
- set ap radio auto-tune max-power 292
- set ap radio channel 293
- set ap radio mode 295
- set ap radio radio-profile 296
- set ap radio tx-power 297
- set ap security 298

set ap upgrade-firmware	300
set arp	109
set arp agingtime	110
set authentication admin	203
set authentication console	206
set authentication dot1x	209
set authentication last-resort	212
set authentication mac	213
set authentication web	215
set auto-config	26
set banner motd	29
set boot backup-configuration	595
set boot configuration-file	596
set boot partition	597
set confirm	29
set dot1x key-tx	519
set dot1x max-req	520
set dot1x quiet-period	520
set dot1x reauth	521
set dot1x reauth-max	522
set dot1x reauth-period	522
set dot1x timeout auth-server	523
set dot1x timeout supplicant	524
set dot1x tx-period	524
set dot1x wep-rekey	525
set dot1x wep-rekey-period	526
set enablepass	19
set fdb	71
set fdb agingtime	72
set igmp	428
set igmp lmqi	429
set igmp mrouter	430
set igmp mrsol	430
set igmp mrsol mrsi	431
set igmp oqi	432
set igmp proxy-report	433
set igmp qi	433
set igmp qri	435
set igmp querier	436
set igmp receiver	436
set igmp rv	437
set interface	111
set interface dhcp-client	112
set interface dhcp-server	113
set interface status	115
set ip alias	115
set ip dns	116
set ip dns domain	117
set ip dns server	118
set ip https server	119
set ip route	120
set ip snmp server	122
set ip ssh	123
set ip ssh server	124
set ip telnet	125
set ip telnet server	126
set length	30
set license	31
set location policy	217
set log	626
set log buffer	626
set log console	626
set log current	626
set log mark	629
set log server	626
set log sessions	626
set log trace	626
set mac-user	221
set mac-user attr	222
set mac-usergroup attr	230
set mobility profile	231
set mobility-domain member	251
set mobility-domain mode member seed-ip	252
set mobility-domain mode seed domain-name	253
set mobility-profile mode	234
set network-domain mode member seed-ip	261
set network-domain mode seed domain-name	263
set network-domain peer	262
set ntp	127
set ntp server	128
set ntp update-interval	129
set port	55
set port name	57
set port negotiation	58
set port speed	60
set port trap	61
set prompt	31
set qos cos-to-dscp-map	91
set qos dscp-to-cos-map	91
set radio-profile active-scan	300

set radio-profile auto-tune channel-config 301
 set radio-profile auto-tune channel-holddown 303
 set radio-profile auto-tune channel-interval 304
 set radio-profile auto-tune power-config 305
 set radio-profile auto-tune power-interval 306
 set radio-profile beacon-interval 307
 set radio-profile countermeasures 307
 set radio-profile dtim-interval 309
 set radio-profile frag-threshold 310
 set radio-profile max-rx-lifetime 311
 set radio-profile max-tx-lifetime 312
 set radio-profile max-voip-bw 313
 set radio-profile max-voip-sessions 315
 set radio-profile mode 316
 set radio-profile preamble-length 320
 set radio-profile qos-mode 321
 set radio-profile rate-enforcement 322
 set radio-profile rts-threshold 323
 set radio-profile service-profile 324
 set radius 503
 set radius client system-ip 506
 set radius deadline 503
 set radius key 503
 set radius retransmit 503
 set radius server 506
 set radius timeout 503
 set rfdetect attack-list 552
 set rfdetect black-list 553
 set rfdetect ignore 554
 set rfdetect log 555
 set rfdetect signature 556
 set rfdetect ssid-list 557
 set rfdetect vendor-list 558
 set security acl 460
 set security acl hit-sample-rate 469
 set security acl ip icmp 460
 set security acl ip ip 460
 set security acl ip tcp 460
 set security acl ip udp 460
 set security acl map 467
 set security l2-restrict 73
 set server group 509
 set server group load-balance 510
 set service-profile active-call-idle-timeout 333
 set service-profile attr 334
 set service-profile auth-dot1x 336
 set service-profile auth-fallthru 337
 set service-profile auth-psk 339
 set service-profile beacon 340
 set service-profile cac-mode 341
 set service-profile cac-session 342
 set service-profile cipher-ccmp 343
 set service-profile cipher-tkip 343
 set service-profile cipher-wep104 344
 set service-profile cipher-wep40 346
 set service-profile cos 347
 set service-profile dhcp-restrict 348
 set service-profile idle-client-probing 349
 set service-profile keep-initial-vlan 350
 set service-profile long-retry-count 351
 set service-profile no-broadcast 351
 set service-profile proxy-arp 353
 set service-profile psk-phrase 354
 set service-profile psk-raw 355
 set service-profile rsn-ie 356
 set service-profile shared-key-auth 357
 set service-profile short-retry-count 358
 set service-profile ssid-name 359
 set service-profile ssid-type 359
 set service-profile static-cos 360
 set service-profile tkip-mc-time 361
 set service-profile transmit-rates 362
 set service-profile user-idle-timeout 365
 set service-profile web-portal-form 366
 set service-profile web-portal-session-timeout 368
 set service-profile wep active-multicast-index 369
 set service-profile wep active-unicast-index 370
 set service-profile wep key-index 371
 set service-profile wpa-ie 372
 set snmp community 130
 set snmp notify profile 132
 set snmp notify target 137
 set snmp protocol 143
 set snmp security 144
 set snmp usm 146
 set snoop 616
 set snoop map 618
 set snoop mode 619
 set summertime 151
 set system contact 32
 set system countrycode 33
 set system idle-timeout 35

set system ip-address 36, 153
 set system location 37
 set system name 38
 set timedate 154
 set timezone 155
 set trace authentication 607
 set trace authentication mac-addr 607
 set trace authentication port 607
 set trace authentication user 607
 set trace authorization 608
 set trace authorization mac-addr 608
 set trace authorization port 608
 set trace authorization user 608
 set trace dot1x 610
 set trace dot1x mac-addr 610
 set trace dot1x port 610
 set trace dot1x user 610
 set trace sm 611
 set trace sm mac-addr 611
 set trace sm port 611
 set trace sm user 611
 set user 235
 set user attr 236
 set user group 237
 set user password 235
 set usergroup 238
 set usergroup attr 238
 set vlan name 74
 set vlan port 75
 set vlan tunnel-affinity 76
 set web-portal 240
 show aaa 240
 show accounting statistics 243
 show ap acl hits 373
 show ap acl map 373
 show ap acl resource-usage 373
 show ap arp 373
 show ap boot-configuration 401
 show ap config 374
 show ap connection 403
 show ap counters 378
 show ap etherstats 386
 show ap fdb 385
 show ap global 405
 show ap group 389
 show ap qos-stats 385
 show ap status 390
 show ap unconfigured 407
 show ap vlan 397
 show arp 156
 show auto-tune attributes 397
 show auto-tune neighbors 399
 show banner motd 39
 show boot 597
 show config 600
 show crypto ca-certificate 494
 show crypto ca-certificate admin 494
 show crypto ca-certificate eap 494
 show crypto certificate 495
 show crypto certificate admin 495
 show crypto certificate eap 495
 show crypto key ssh 497
 show dhcp-client 157
 show dhcp-server 159
 show dot1x 526
 show fdb 77
 show fdb agingtime 79
 show fdb count 80
 show igmp 438
 show igmp mrouter 443
 show igmp querier 444
 show igmp receiver-table 446
 show igmp statistics 448
 show interface 161
 show ip alias 163
 show ip dns 164
 show ip https 165
 show ip route 167
 show ip telnet 169
 show license 39
 show load 39
 show location policy 246
 show log buffer 630
 show log config 632
 show log trace 633
 show mobility-domain 254
 show mobility-domain config 254
 show mobility-profile 247
 show network-domain 263
 show ntp 170

show port counters 62
show port status 63
show qos 92
show qos default 93
show qos dscp-table 93
show radio-profile 408
show rfdetect attack-list 559
show rfdetect black-list 559
show rfdetect clients 560
show rfdetect countermeasures 563
show rfdetect counters 564
show rfdetect data 566
show rfdetect ignore 568
show rfdetect mobility-domain 568
show rfdetect ssid-list 573
show rfdetect vendor-list 573
show rfdetect visible 574
show roaming station 81
show roaming vlan 83
show security acl 470
show security acl editbuffer 470, 471
show security acl hits 472
show security acl info 473
show security acl map 474
show security acl resource-usage 475
show security l2-restrict 84
show service-profile 413
show service-profile cac session 422
show sessions 534
show sessions network 536
show snmp community 173
show snmp counters 173
show snmp notify profile 173
show snmp notify target 174
show snmp status 174
show snmp usm 175
show snoop 620
show snoop info 621
show snoop map 621
show snoop stats 622
show summertime 175
show system 40
show tech-support 44
show timedate 176
show timezone 177
show trace 611

show tunnel 85
show version 602
show vlan config 86
show voip max-sessions 423
show voip summary 424

T

telnet 177
traceroute 179

UNIVERGE WL
Command Reference (V1)

NWA-027517-001

May, 2007 ISSUE 1.0

Publishing Office NEC Infrontia Corporation
Data Wireless Networks Division

© 2007 NEC Infrontia Corporation

Notice

- (1) All right reserved.
- (2) The contents of this manual is subject to change without notice.

Printed in Japan
0705-010

